CENTRO UNIVERSITÁRIO ANTONIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A LEI GERAL DE PROTEÇÃO DE DADOS E OS IMPACTOS JURIDICOS NA ERA DIGITAL

Paloma Monique Campos Carneiro

Presidente Prudente/SP

2022

CENTRO UNIVERSITÁRIO ANTONIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A LEI GERAL DE PROTEÇÃO DE DADOS E OS IMPACTOS JURIDICOS NA ERA DIGITAL

Paloma Monique Campos Carneiro

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito sob orientação da Professora Doutora Gisele Caversan Beltrami Marcato.

Presidente Prudente/SP

2022

A LEI GERAL DE PROTEÇÃO DE DADOS E OS IMPACTOS JURIDICOS NA ERA DIGITAL

Monografia aprovada como requisito parcial para obtenção do Grau de Bacharel em Direito.

Paloma Monique Campos Carneiro
Orientadora: Gisele Caversan Beltrami Marcato.

DEDICATÓRIA

Somente através de ajuda e incentivo foi possível a conclusão deste trabalho. Sem sombra de duvidas dedico esta monografia a minha família, em especial meus pais que são pilares da minha formação como ser humano, e aos meus amigos, que a cada tropeço, a cada pensamento de desistir, seguraram em minha mão e me conduziram para prosseguir no caminho da conclusão. Sozinha, não seria possível. Esta monografia é a prova de que todo investimento e dedicação valeram a pena.

Artigo III
Fica decretado que, a partir deste instante,
haverá girassóis em todas as janelas,
que os girassóis terão direito
a abrir-se dentro da sombra;
e que as janelas devem
permanecer, o dia inteiro,
abertas para o verde onde cresce a esperança.
Artigo VII
Por decreto irrevogável fica
estabelecido o reinado permanente
da justiça e da claridade, e a
alegria será uma bandeira generosa
para sempre desfraldada na alma
do povo.
Os Estatutos do Homem

(Ato Institucional Permanente)

Thiago de Mello

AGRADECIMENTOS

Agradeço a Deus por permitir que esse sonho se torna realidade, por me fortalecer enquanto ser humano, por me proporcionar entendimento e compreensão na condução deste trabalho.

Agradeço a minha família, que são meus pilares enquanto ser humano, enquanto profissional, e foram grandes incentivadores quando decidi ingressar em uma segunda graduação.

Agradeço aos meus amigos, que toleraram cada dia de estresse e angustia, mas que também celebraram a cada capitulo que fora concluído desta obra.

Agradeço a minha orientadora, que me ensinou que é possível realizar um trabalho dessa responsabilidade, com correções respeitosas e que ensejavam o desejo de escrever cada vez melhor, mas acima de tudo, que quando desanimava sem ela saber, com suas palavras e correções, me fazia sentir forte pra continuar.

RESUMO

O presente estudo tem por objetivo realizar uma análise acerca da normativa 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD). A problemática da pesquisa esboça a necessidade de implementação de uma normativa com proteção jurídica direcionada aos dados dos indivíduos, com destaque especial, os dados extraídos de mídias digitais. Um dos resultados da pesquisa, versa sobre a compreensão do cenário político e jurídico que a referida normativa ocasionou ao adentrar no ordenamento jurídico brasileiro, nos impactos relacionais ocasionados entre Brasil e demais países, em especial os que compõem a União Europeia. No discorrer da problemática evidenciou-se a necessidade de delimitar a pesquisa para discussões pautadas na forma como a LGPD direciona o tratamento de dados resultante de mídias digitais, visto que a sociedade contemporânea está caracterizada por uma sociedade informacional. A questão a ser discutida é de interesse jurídico, visto que permeia sobre a segurança jurídica nesse cenário. Sendo assim, este estudo aborda discussões sobre uma normativa moderna, embora exista no Brasil Leis desde meados da década de 1980 com essa temática, foi somente na sociedade contemporânea que a proteção de dados atingiu um status de reconhecimento, de modo que o próprio Supremo Tribunal de Justiça qualificou essa proteção como um direito fundamental, com previsão no artigo 5º da Constituição Federal de 1988, tornando assim cláusula pétrea.

Palavras Chaves: Lei Geral de Proteção de Dados. Mídias Digitais. Direito Fundamental. Segurança Jurídica.

ABSTRACT

The present study aims to carry out an analysis of the regulation 13.709/2018, known as the General Data Protection Law (LGPD). The research problem outlines the need to implement a regulation with legal protection directed to the data of individuals, with special emphasis, the data extracted from digital media. One of the results of the research deals with the understanding of the political and legal scenario that the aforementioned normative caused when entering the Brazilian legal system, with emphasis on the way in which it was built, and the relational impacts caused between Brazil and other countries, especially those that make up the European Union. In discussing the problem, it became evident the need to delimit the research for discussions based on the way in which the LGPD directs the treatment of data resulting from digital media, since contemporary society is characterized by an informational society. The issue to be discussed is of legal interest, as it permeates legal certainty in this scenario. The present study deals with a modern regulation, although laws exist in Brazil since the mid-1980s, it was only in contemporary society that data protection reached a status of recognition, so that the Supreme Court of Justice itself qualified this protection as a fundamental right, provided for in article 5 of the Federal Constitution of 1988, thus making it a stony clause.

Keywords: General Data Protection Law. Digital Media. Fundamental right. Legal Security.

LISTA DE ILUSTRAÇÕES, TABELAS E QUADROS

FIGURA

QUADRO

SUMÁRI
O

1 INTRODUÇÃO

A sociedade contemporânea vem avançando na esfera tecnológica cada dia mais, as relações humanas que antes se materializavam somente presencial, hoje podem ser estendidas a quilômetros de distância com o apoio das mídias digitas. Ocorre que, para acesso a essas plataformas há necessidade de exposição de dados pessoais para assim ser realizado os devidos contatos, contudo esse momento é propicio para o armazenamento de dados, de cunho pessoal, o que estava ocasionando a criação de uma base de informações pessoais utilizadas em transições pautadas na economia on-line.

Com essa alteração desenfreada na sociedade moderna, os legisladores entenderam se fazer necessário um instrumento que acompanhassem esses avanços na sociedade digital, de forma que limitasse e protegessem os dados dos usuários dessas plataformas, surgindo assim a Lei Geral de Proteção de Dados – LGPD.

Com base nessa problemática o presente estudo teve por objetivo, esboçar questões introdutórias a respeito da LGPD, tendo como eixo principal a proteção dos dados pessoais, e os direcionamentos da aquisição dessas informações, bem como, visa permear reflexões a respeito da maneira como essa normativa, abordará a proteção de dados de pessoas físicas ou jurídicas.

Cabe um destaque no que diz respeito ao tempo de existência da legislação supracitada, visto que a mesma, adentrou ao ordenamento jurídico brasileiro em setembro do ano de 2020 (dois mil e vinte), e impactou as relações horizontais e verticais da sociedade contemporânea em um curto espaço de tempo, afetando em especial as relações jurídicas.

Dentre as diversas alterações Além da proteção dos dados acessados nessas plataformas, a LGPD determinou que se criasse um instrumento que autorizasse a coleta e compartilhamentos das informações dos usuários, no instante em que o mesmo acessasse essas mídias, conhecido como consentimento, visto que se torna fundamental que cada indivíduo tenha clareza e expresse de forma objetiva a autorização na coleta e manuseio de seus dados pessoais.

Diante do exposto o referido estudo discorre no segundo capitulo o contexto social e politico em que a LGPD se consolidou, com destaque no cenário de uma sociedade marcada pela informação e informatização, que proporciona acessos em números imensuráveis de indivíduos, permitindo assim que as relações sociais, jurídicas e políticas sejam moldadas a partir do momento em que esses indivíduos acessam esse

círculo informacional. Ainda dentro do segundo capitulo foi possível discorrer sobre a sociedade pós moderna, também conhecida como sociedade 4.0, marcada pela tecnologia da informação, e por fim para compreensão da LGPD em sua totalidade, nesse segundo capitulo foi esboçado sobre a proteção de dados no Direito Comparado com destaque nas contribuições da Corte Europeia (Europa) EUA e como essas contribuições influenciaram na Trajetória Histórica da LGPD no Brasil.

No terceiro capitulo, fora explanado o Conceito de Privacidade na Era Digital onde foi possível esclarecer a relação de privacidade, com a intimidade e a liberdade dos indivíduos, sendo possível apresentar diversos documentos e aparatos normativos de outros países que contribuíram para a construção de reflexões acerca do tema, com destaque na Convenção Europeia dos Direitos do Homem, na Declaração Universal dos Direitos Humanos, bem como artigos publicados na Harvard Law Review, Right to privacy, entre outros. Ainda no terceiro capitulo, fora discorrido sobre os princípios aplicáveis no âmbito da privacidade, em especial os cinco princípios éticos presentes na Carta da União Europeia que são utilizados na regulamentação das relações referente a inteligência artificial, a qual é possível estender para a proteção de dados dos indivíduos. Por fim, abordou-se a proteção de dados como um mecanismo para cessar ou minimizar a comercialização dessas informações, encerrando-se com os impactos diretos da LGPD nos negócios jurídicos na era digital.

No quarto capitulo foi possível apresentar algumas experiencias e jurisprudências brasileiras no que diz respeito a materialidade da LGPD nos tribunais brasileiros e as transformações no ordenamento jurídico brasileiro. Além das experiências, foi possível apresentar uma linha do tempo referente a trajetória da LGPD. Por fim nesse capitulo, fora explanado o entendimento da STF no que diz respeito com destaque na Emenda Constitucional 115 de 2022, a qual possibilitou a efetividade da Proteção de Dados como Direito Fundamental, com previsão de clausula pétrea.

Desta forma para fundamentação do estudo, a referida pesquisa abordou o método dedutivo com a finalidade de verificar as mudanças ocorridas com o consentimento da distinta Lei. Foram utilizados de pesquisas eletrônicas, artigos, dissertações de mestrado e monografias a respeito da temática, bem como, aparatos literários e normativos.

2 CONTEXTO SOCIAL E POLITICO DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Quando mensuramos a Lei Geral de Proteção de Dados, também conhecida pela sigla LGPD, se torna imprescindível contextualizar a mesma no cenário social e político da sociedade contemporânea, visto que ambos têm relação direta no comportamento dos indivíduos sociais.

A LGPD de forma genérica pode ser compreendida como uma ferramenta de tutela de proteção dos dados pessoais de cada indivíduo, ainda que já existiam aparatos normativos que regulassem a proteção de dados em nosso País, como Constituição Federal de 1988, Código Civil, Código de Defesa do Consumidor, etc, ainda assim com o crescimento considerável da sociedade tecnológica, tornou-se necessário um aparato normativo especifico para regular essas relações, surgindo então a primeira Lei Nacional sobre o tema, a LGPD a qual disciplina sobre:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018).

Atualmente vivemos o que se fala em *internet sem barreiras*, a qual tem influenciado no comportamento de toda uma sociedade, proporcionando grandes impactos em diversos âmbitos, com ênfase nos relacionais, influenciando diretamente na comunicação entre indivíduos para com indivíduos, bem como, entre objetos e indivíduos.

Com o avanço acentuado da era digital, a internet tem proporcionado que os meios relacionais e de comunicação se tornem cada vez mais acessível, diminuindo assim a distância de comunicação entre as partes. Embora vivenciemos uma escala geográfica imensurável do desenvolvimento de tecnologias no âmbito da internet, ainda assim, torna-se fundamental que os indivíduos possuam segurança no manuseio dessas tecnologias, e segurança esta que será abordada como a segurança jurídica[1], tornando-se fundamental a intervenção do direito nessas relações.

[1] A concepção de segurança vem atrelada a organização jurídica, bem como, ao direito, desde o início da civilização, buscando garantir uma boa convivência entre os seres [1]. Como exemplo de sua importância no período histórico, pode-se dizer que essa segurança tem os seus primeiros aparecimentos já na Declaração dos Direitos do Homem e do Cidadão.

A sociedade contemporânea está marcada por ser uma sociedade de informação e informatização, acessada por um número imensurável de indivíduos, permitindo assim que as relações sociais, jurídicas e políticas sejam moldadas a partir do momento em que acessam esse círculo informacional e seja produzido conteúdos acerca dos acessos.

Ocorre que essa sociedade informacional, é acessada por qualquer indivíduo com que manuseei a internet, o que possibilita um armazenamento de informações de forma involuntária pelo individuo que o acessa. As maquinas de armazenamento dessas informações digitais, via de regra se encontram presente nos programas de computadores,e atualmente nos aparelhos de smartphones, e também conhecidos aparelho celular.

O acesso gratuito à internet e as informações digitais, nos apresenta como algo gratuito, entretanto quando realizada uma analise mais profunda, compreende-se que nada mais é que um modelo de negócio, como bem explana Krieger (2019, pag. 22)

> Ao passo que a Internet possui um modelo de negócio em que o acesso é "gratuito", isto é, no qual não há prestação pecuniária por aqueles que a utilizam, enganam-se aqueles que acreditam que a ferramenta não retira nada de seus usuários. Como troca de seus bens de consumo fornecidos, a Internet utiliza dos dados pessoais dos seus "consumidores", em troca da mencionada publicidade direcionada. Desse modo, o consumidor torna-se também uma parte do produto comercializado, tendo em vista que são seus próprios dados que direcionam a economia em questão.

O acesso a internet, não é um mecanismo benevolente, o que seria contraditório diante de uma sociedade capitalista, o acesso a internet permite que as redes sociais extraiam informações em cada site acessado, em cada página clicada, em cada perfil criado nas redes sociais como *facebook, instagram, contas de email, twiter,* etc, e a partir do momento do click sem que o usuário tenha compreensão uma série de informações já estão sendo extraídas dos seus acessos, o que possibilita ser realizado o que chama-se de publicidades direcionadas, de acordo com o perfil formulado com as informações de acessos daquele usuário.

Um exemplo simples, ocorre quando realizamos uma pesquisa sobre um determinado eletrodoméstico. A partir dessa pesquisa, quando formos realizar outras pesquisas, sempre aparecerá anúncios, ou noticias sobre equipamentos que já havíamos pesquisados, nesse caso um eletrodoméstico.

Em síntese, conclui-se que cada rede social, cada acesso realizado pelos usuários, permite que se crie um perfil de informações daquele usuário, e não se reduz somente ao uso de computadores, mas também aos smartphones que se tornou um equipamento intrínseco ao cotidiano do ser humano.

Para compreendermos melhor todo esse contexto subjetivo, a autora Krieger (2019, p.25), apresenta um exemplo real desse monitoramento de dados e informações:

> Para ilustrar o cenário, segundo pesquisa dos britânicos pertencentes à ONG que analisa o controle dos dados na Internet (Privacy Internacional) 12, recentemente descobriu-se que aplicativos de controle de ciclo menstrual estariam compartilhando dados de sua rede (como dados de saúde e da vida sexual das usuárias, dentre outras informações) para a plataforma do Facebook.

Se a violação de uma correspondência já é caracterizada em nosso ordenamento jurídico como um ato ilícito, o manuseio e compartilhamento de informações pessoais dos indivíduos, em meio digital, não seria diferente.

Ainda que pareça uma critica referente a coleta de dados e informações através das mídias digitais, a crítica em si não se pauta nisso, mas sim na utilização dos dados, esses dados não podem ser utilizados para maleficio da sociedade, ao contrário, a utilização dessa ferramenta pode ser construída como algo benéfico, desde que os titulares das informações tenham consciência e autorizem o devido uso.

Alguns autores compreendem os dados pessoais como o novo petróleo do século XXI,

> Vistos já como o novo petróleo, os dados são hoje insumos essenciais para praticamente todas as atividades econômicas e tornaram-se, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão data-driven economy, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek, o capitalismo do século XXI passou a centra-se na extração e no uso de dados pessoais.(FRAZÃO, 2019, p.07)

A extensão desses dados se apresenta tão subjetivo, tornando-se imensurável, ressaltando a importância de um tratamento seguro dessas informações, destacando que não acarreta em impactos apenas na área econômica, mais também nas questões políticas e sociais. Esses impactos podem ser negativos e positivos, tudo irá depender de como se iniciara a coleta, manuseio e a finalidade de aquisição dessas informações, ou seja, o devido direcionamento.

Embora que para muitos, a LGPD tenha por materialidade a construção de um sistema burocrático que dificulta a engrenagem do direcionamento dos dados e informações adquiridas, caminhar em velocidade mais assídua, ainda assim a burocracia possibilita uma engrenagem segura, pelos caminhos ideais.

Desta forma, a coleta e o manuseio de dados de uma sociedade dever ser extraído de modo que aquele que será impactado de forma direta ou indireta tenha consciência e

realize as devidas autorizações de forma compreensível sobre o manuseio desses dados, também conhecido como consentimento.

A área politica também possui acesso a esses dados produzidos pelo que conhecemos de algoritmos, onde possibilita compreender um perfil dos cidadãos "tudo isso acontece por meio de um monitoramento e vigília constantes sobre cada passo da vida das pessoas, o que leva a um verdadeiro capitalismo de vigilância, cuja principal consequência é a constituição de uma sociedade também de vigilância" (FRAZÃO, 2019, p. 10). Frazão, utiliza a expressão vigilância, no sentido de termos nos tornado uma sociedade que está constantemente sendo monitorada, e controlada.

Diante disso, entendendo que se trata de um avanço tecnológico e com comportamentos e resultados subjetivos, a proteção jurídica necessita se fazer presente para regular a utilização e o manuseio desses dados, de modo que seja garantido os princípios e direitos fundamentais da privacidade e autonomia de vontade através do consentimento.

No próximo item será realizado uma breve reflexão sobre a consolidação da LGPD em uma sociedade pós revolução industrial, marcada pelo avanço tecnológico.

2.1 A sociedade Pós-moderna - 4.0

A sociedade pós moderna, também conhecida como sociedade 4.0 é marcada pela tecnologia da informação. A informação não possui uma restrição de acesso, e esta intrinsicamente ligada a liberdade, seja de acesso seja de divulgação. A Constituição Federal de 1988 prevê, em seu artigo 5º, inciso XIV, que "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional". Ou seja, o referido artigo trata do acesso à informação em âmbito liberal, mas com algumas limitações.

O que vivemos atualmente, na sociedade contemporânea, são os reflexos e resultados das construções e desdobramento da revolução industrial, em que nesse período, ocorreu um vasto aprimoramento dos meios de comunicação, como bem pontua Santi (2020, pag.21):

> Nota-se que, a sociedade da informação é considerada uma forma de evolução dos meios de comunicação perante a tecnologia digital. São inovações tecnológicas que armazenam dados pessoais que se tornam básicos e muitas vezes essenciais para que o cidadão titular dos dados pessoais possa exercer sua autodeterminação informativa [...]

A sociedade contemporânea é marcada pela globalização, que vem contribuindo e ganhando cada vez mais espaço nos aplicativos e acesso aos meios digitais de uma forma massificada, proporcionando um grande avanço na tecnologia digital, bem como, o acesso direto aos dados pessoais dos indivíduos que acessam mecanismos tecnológicos ligados a informação.

> [...] com a revolução tecnológica, as inovações são desenvolvidas em velocidade exponencial, em formas jamais antes presenciadas. Junto ao desenvolvimento da informática, a informação tornou-se facilmente difundida, e, portanto, criada e reproduzida com alta rotatividade. O direito, por outro lado, encontra dificuldades em acompanhar as mudanças da sociedade informacional, obrigando-se a se adaptar às novas formas de relações sociais e jurídicas. Assim como a revolução tecnológica trouxe uma necessidade econômico social da proteção de bens imateriais, se observará que a revolução da informática trouxe a necessidade da imposição de limites éticos a coleta, utilização e distribuição de informações pessoais. (PANE, 2019, p. 08).

Com a revolução tecnológica e suas múltiplas inovações, ocorreu uma vasta expansão e acesso pelos indivíduos societários, proporcionando que a sociedade tenha uma maior interação entre indivíduo e objetos.

Além do acesso, há também um interesse imensurável, onde o indivíduo acessa informações sem barreiras que o limite, tornando cada vez mais fácil e democrático o acesso as mídias digitais. Ocorre que o fato de não possuir barreiras gera uma preocupação, em especial na esfera jurídica, onde torna-se subjetivo a manutenção e proteção dos direitos fundamentais dos indivíduos sociais.

Desta forma, compreende-se que os acessos desenfreados e sem fronteiras, a tecnologia da informação e suas ferramentas, necessitam de respaldos normativos, visto que, cada acesso de um indivíduo em uma determinada mídia digital, possibilita que essa mídia adquira diversas informações desse individuo sem que o mesmo perceba, construindo assim uma base de dados e informações que podem ser compartilhadas e muitas vezes comercializadas.

Visto o que foi brevemente explanado, tornou-se necessário a implantação de uma normativa especifica que regularizasse, o acesso à informação sem violação dos direitos fundamentais, surgindo então a LGPD. O que era compreendido como uma opção a proteção de dados, com a chegada dessa normativa, tornou-se uma obrigação, implicando na restruturação de diversas empresas e organizações, ainda que a sensibilidade e a provocação por essa readequação tenham um fator preponderante e incentivados: as multas.

Com base em um fenômeno multinacional, a LGPD sofre fortes influencias de normativas de outros países, como por exemplo o Regulamento Geral sobre a Proteção de Dados - RGPD:

> [...] foi sancionado o texto que trata do uso de informações pessoais de modo específico no ordenamento nacional, visando desenvolver a proteção da privacidade no meio eletrônico. Com o período de vacatio legis de 18 meses, a nova Lei Geral de Proteção de Dados (LGPD) passa a ter eficácia plena em todo território nacional em fevereiro de 2020, consagrando princípios e garantias semelhantes àqueles do Regulamento europeu e reforçando, ainda, o controle do titular sobre seus dados pessoais pela exigência do consentimento, o direito ao acesso e à informação, o direito de retificação e apagamento. Dispõe sobre o modo pelo qual informações pessoais podem ser coletadas e tratadas, seja a partir de cadastros, no fechamento de compras ou até mesmo em imagens publicadas, estabelecendo requisitos para que esses dados possam ser tratados, repassados, publicados e até comercializados. (SOUZA, 2018, p. 46).

Esse Regulamento tem origem na União Europeia e tem como objeto a proteção dos dados e informações pessoais de cada indivíduo residente na Europa. O Brasil infelizmente não foi o primeiro país a elaborar uma normativa que regulasse especificamente a proteção de dados dos indivíduos.

O próximo item irá abordar a relação direta entre a LGPD com as normativas europeias no que diz respeito a proteção de dados.

2.2 Proteção de Dados no Direito Comparado: Corte Europeia (Europa) X EUA

A LGPD possui origem normativa na Europa, precisamente na Alemanha, por volta da década de 1970-1980, e se tornou necessária pois nesse momento a sociedade estava passando por uma grande transformação na área da comunicação, visto que estava chegando a era da computação, esboçando assim, o início de uma era digital.

A era digital nesse período ainda estava desconhecida, o que se sabia é que uma máquina poderia ser utilizada como ferramenta de comunicação instantânea, além de permitir compartilhar documentos. Desta forma o judiciário se viu diante de uma inovação sem controle, ou seja, havia possibilidades de trocar informações de modo que o âmbito jurídico não conseguiria acessa-las e assim regular essas relações horizontais, surgindo a necessidade de mecanismos que regulassem essas relações de forma vertical, com a proteção do Estado**.**

No Brasil, é notório a quantidade de aparatos normativos esparsos que foram surgindo e permitindo o cuidado com a privacidade enquanto direito fundamental, do sigilo de fonte, etc. Entretanto cada Lei que discorre em seu texto formas sobre a proteção da integridade dos indivíduos, deixam lacunas que não trabalhassem especificamente sobre a proteção de dados e informações de uma determinada pessoa.

No ano de 2014, tivemos sancionada no ordenamento jurídico Brasileiro a normativa 12.965/14 que regula especificamente o manuseio da internet, desta forma ficou conhecido como o Marco Civil da Internet. Ainda assim, uma normativa como essa de cunho inovador e tecnológico, abrange os crimes cibernéticos, e não a proteção de dados dos indivíduos que circulam pelas mídias digitais, permitindo assim uma lacuna que deveria ser sanada pelo direito.

Ocorre que esse fenômeno de inovação tecnológica e necessidade de proteção não estava acontecendo somente no Brasil, mas se trata de um fenômeno que estava acontecendo no mundo todo, afinal a internet permite esse avanço desenfreado e sem barreira, em momentos concomitantes. Um exemplo dessa inovação tecnológica normativa é o General Data Protection Regulation – GDPR – Regulamento Geral da Proteção de Dados, que objetiva a proteção de dados dos cidadãos da União Europeia:

> O Regulamento alerta para o aumento exponencial do tratamento de dados pessoais associado ao desenvolvimento dastecnologias de informação e à necessidade de adaptação de seus princípios a um mundo que cada vez mais depende da coleta e do tratamento de dados na Internet e fora dela. Mostra, ainda, a necessidade de harmonizar a Privacy Shield). O Japão e a Coréia do Sul estão sob análise da Comissão e, a depender do resultado, poderão ser objeto de decisão de adequação no porvir. crescente utilidade e conveniência de tratamento desses dados com as liberdades e direitos fundamentais, tendo por objetivo reforçar e unificar a proteção de dados pessoais na União Europeia (UE), especificando direitos e obrigações correspondentes. Exemplo disso é a própria definição de dado pessoal, que se mostra muito mais detalhada, tratando com tal aquele cuja informação seja relativa a uma pessoa singular identificada ou identificável -titular dos dados, sendo considerada identificável todos aqueles que possam ser identificados, direta ou indiretamente, em especial por referência a um identificador, que pode ser um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular. (SOUZA, 2018, p. 50)

Esse regulamento faz menção e discorre sobre a proteção dos dados de forma minuciosa, apresentando que um individuo é marcado por dados de natureza numérica, psíquica e ate mesmo social, e pode ser facilmente identificado de acordo com as mídias digitais acessados por esses usuários.

O que se tem discorrido no texto normativo da LGPD no que diz respeito a licitude do tratamento de informações dos dados dos usuários, bem como através do livre consentimento e transparência, tem herança que prevê o artigo 5º da GDPR:

> Art. 5 GDPRPrinciples relating to processing of personal data
> Personal data shall be:
> processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
> collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
> adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
> accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
> kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
> processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).[2]

O Regulamento deixa expressamente claro em seus princípios que a finalidade da aquisição de dados e informações devem ser proporcionais as necessidades reais, e

[2] Arte. 5 RGPDPrincípios relativos ao processamento de dados pessoais
Os dados pessoais devem ser: tratados de forma lícita, justa e transparente em relação ao titular dos dados («licitude, equidade e transparência»);coletados para fins específicos, explícitos e legítimos e não processados de maneira incompatível com esses fins; O tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos não deve, nos termos do artigo 89.º, n.º 1, ser considerado incompatível com os fins iniciais («limitação da finalidade»); adequados, relevantes e limitados ao necessário em relação às finalidades para as quais são processados («minimização de dados»); precisos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para garantir que os dados pessoais inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora («exactidão»); mantidos de uma forma que permita a identificação dos titulares dos dados por não mais do que o necessário para as finalidades para as quais os dados pessoais são processados; os dados pessoais podem ser armazenados por períodos mais longos, na medida em que os dados pessoais sejam processados exclusivamente para fins de arquivamento de interesse público, para fins de pesquisa científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeito à implementação das medidas técnicas e organizacionais adequadas medidas exigidas pelo presente regulamento para salvaguardar os direitos e liberdades do titular dos dados («limitação de armazenamento»);
processados de maneira a garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas ('integridade e confidencialidade').
O responsável pelo tratamento deve ser responsável e poder demonstrar o cumprimento do n.º 1 («responsabilização»).

deve acontecer de forma transparente, de modo que o usuário tenha clareza dessa utilização e clareza da finalidade, respeitando sempre o princípio que entendemos em nosso ordenamento de princípio da proporcionalidade entre a aquisição de informações, quantidade e tempo de armazenamento.

Outro instituto interessante a ser citado, diz respeito ao consentimento dos indivíduos para com a aquisição e o manuseio desses dados, presentes no artigo *6º da GDPR*, "estabelece que o tratamento somente será lícito e legítimo se o titular dos dados tiver dado o seu consentimento específico para o tratamento dos seus dados pessoais. De forma complementar, assegura o direito de revogação do consentimento a qualquer momento [...] (SOUZA, 2018, p. 52)

A privacidade e o consentimento tornam-se eixos principais no referido documento, e mais rigoroso em especial no que diz respeito a revogação do consentimento a qualquer tempo, e o mesmo deve ser manifesto de forma clara e explicita, não se aceitando a frase que nós brasileiros utilizamos: "o silencio representa anuência".

O que se torna interessante destacar, como já foi citado anteriormente, a GDPR influenciou diversos países na elaboração de normativas que abordassem a proteção de dados, mas o que estimulou a implantação da normativa de proteção de dados em diversos países , foi que a União Europeia determinou que somente iria se relacionar com países que estivessem adeptos a aparatos legais que regulasse a referida proteção.

Destaca-se que a LGPD é uma normativa jurídica, e o âmbito jurídico necessita acompanhar essas mudanças e inovações, tendo compreensão doutrinária e jurídica da pratica e aplicação da normativa. Destaca-se que a LGPD não possui uma abrangência no que diz respeito especificamente a coleta de dados através das mídias digitais, como por exemplo a utilização dos *cookies*, surgindo assim a necessidade de normativas reguladoras que abranja especificamente esse meio de aquisição de dados, ou seja, há necessidade de delimitar e especificar cada vez mais a coleta e tratamento de dados, especificamente aqueles coletados através de ferramentas digitais, como site diversos.

2.3 Trajetória Histórica da LGPD no Brasil

No Brasil, o primeiro esboço no que diz respeito a proteção de dados, apareceu na Constituição Federal de 1988, com destaque no Artigo 5º, "X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;" esse texto

possibilitou surgimento de outros aparatos que regulassem e compreendessem a importância de proteger as informações pessoais dos indivíduos, surgindo assim a Lei 9.296 de 1996 (em vigência) que trata sobre as interceptações telefônicas e a violação de correspondências, com ressalvas quando se trata de investigação criminal.

Até a chegada da LGPD vários outros aparatos normativos foram criados, objetivando a proteção integral dos dados dos indivíduos, como o Código de Defesa do Consumidor, sempre visando manter a equidade e proteção da parte mais vulnerável frente a um negócio jurídico.

Ressalta-se que a LGPD se trata de uma Lei especifica que aborda sobre o tratamento de dados, entretanto, não é a primeira Lei no ordenamento jurídico brasileiro que trata sobre a proteção da privacidade do indivíduo.

No Código Penal de 1940 já existia esboços sobre o tratamento de dados e penalidades referente a violação da privacidade, especificamente no que previa o artigo 151 do referido aparato normativo: "Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena - detenção, de um a seis meses, ou multa."

O distinto artigo não esboça sobre a proteção de dados, mas é claro no que diz respeito a sanção daquele que violar correspondência, o que está relacionado ao direito à privacidade. O código penal foi promulgado em 1940, e por tratar da violação da privacidade do indivíduo, podemos compreender que a normativa se caracteriza como um embrião no que diz respeito a proteção da privacidade, informação e dados dos indivíduos.

Mais adiante em 1988, foi promulgada nossa carta magna, a Constituição Federal de 1988, e nela contem esboços sobre a proteção de dados:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Somente na década de 1990 que surge então a primeira Lei que tratou explicitamente sobre a proteção de dados dos indivíduos sociais:

> A primeira lei brasileira a de fato tratar da proteção de dados e direitos relativos a este é o Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990 ("CDC"). O dispositivo regula as relações entre consumidores e fornecedores, estabelecendo obrigações e direitos para ambos os lados. Os dados consumeristas são tema do artigo 43, que dá aos consumidores o direito de ter acesso e a corrigir informações referentes a si mesmo, entre outras disposições. O CDC foi complementado pela Lei do Cadastro Positivo, Lei 12.414/2012, que criou um microssistema de proteção de dados no contexto das relações de consumo, mais especificamente dados de adimplência e modelagem de crédito, e trata sobre temas como princípio da finalidade, necessidade e até mesmo de revisão de decisões automatizadas. (SOUZA, 2018, p. 15)

O Código de Defesa do Consumidor (CDC), trata sobre o acesso a informações, destinado aos consumidores de algum produto, disciplina a proteção de dados pessoais, conforme exposto no artigo 2º do CDC[3], os incisos presentes no artigo 2º do CDC tratam-se de princípios que norteiam a proteção de dados, e esses princípios embasaram e se fazem presente na própria LGPD.

Quando se faz uma analise minuciosa da Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor é possível identificar diversas semelhanças, o que difere explicitamente é que o CDC regulamenta a relação entre Fornecedor e Consumidor enquanto a LGPD é destinada a todos independente de relação de consumo.

A partir dessas Leis mencionadas, outras diversas Leis e Resoluções foram sendo criadas, afim de proteger os dados dos indivíduos, como por exemplo a Lei n° 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann, que trouxe em seu enredo a tipificação dos crimes informáticos.

Mais adiante, é promulgada a Lei n° 12.527, de 18 de novembro de 2011, que versa sobre uma gestão transparente do poder público, nas três esferas de governo, proporcionando a sociedade o acesso a informação, em especial no que diz respeito a destinação de verbas, e demais custeio no âmbito do setor público.

Um grande marco, que se faz necessário ser citado nessa trajetória de aparatos normativos que disciplinam a proteção de dados e o direito ao acesso a informações seguras, foi a Lei 12.965, de 23 de abril de 2014, também conhecido como Marco Civil

[3] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

da Internet, a qual "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil."

Essa Lei obteve uma construção diferenciada visto que, no decorrer da elaboração do Texto Legislativo, foi proporcionado espaços para participação direta da população brasileira através das audiências públicas. A participação popular na construção do Marco Civil da Internet, também tem uma interessante relação com a construção da LGPD, visto que a mesma iniciou seus esboços do texto normativo no ano de 2010, onde fora construído um site referente a proteção de dados, e disponibilizado uma consulta pública para toda a população sobre o que se tratava o assunto: Proteção de Dados:

> A consulta, que teve duração de 4 meses, recebeu comentários de diferentes setores da sociedade, formando assim um contingente multissetorial de contribuições. Vale ressaltar que, à época, este anteprojeto foi bastante associado à discussão pública acerca do Marco Civil da Internet, naquele momento ainda em processo de debate, recebendo algumas vezes, por esse motivo, o nome de "Marco Legal da Proteção de Dados"29. Com os primeiros comentários ao APLPD, foi feito um esboço do que viria a se tornar o futuro texto da LGPD, 8 anos mais tarde. (MONTEIRO, Renato Leite. GOMES, Mari Cecilia Oliveira. NOVAES, Adriane Loureiro , MORIBE, Gabriela. CAMARA, Dennys Eduardo Gonsales. GHERINI, Pamela Michelena De Marchi. 2018, pag.10)

Logo se vê que se trata de uma Lei história, visto que até a forma de sua construção fora diferenciada, onde escutou e permitiu que a população opinasse a respeito da temática, o que de fato os principais interessados são os cidadãos, a coerência é permitir voz na construção de uma Lei que tem como objeto de proteção os dados dos indivíduos.

Em seguida, como grande marco também, surge a LGPD (2018-2020) visando proteger a base de dados dos indivíduos na era digital. Em décadas anteriores, os negócios jurídicos eram realizados frente a frente, com uso do papel físico, impresso, hoje, essas relações e negociações passaram por uma grande transformação, sendo realizadas através do ambiente virtual, impactando inclusive na maneira como a sociedade se relaciona.

Ocorre que, muitas vezes o indivíduo, usuário de um sistema digital, muitas vezes concede informações a um banco de dados *on line* sem ao menos possuir consciência do feito, fornecendo dados de forma involuntária.

Quando ocorre esse fornecimento de dados, ainda que involuntariamente e sem ao menos uma previa "autorização", essas informações não param de ser compartilhas, acessadas por outros bancos de dados, e muitas vezes vendidas.

Quantas vezes pesquisamos um determinado produto na internet, e em seguida começa a aparecer vários anúncios sobre aquele produto pesquisado. Sem sombra de dúvidas não é magica, é o que conhecemos por cookies, onde esta ferramenta armazena e rastreia todas as pesquisas, ou seja, a todo momento o indivíduo que faz uso das ferramentas digitais está sendo monitorado, a ponto de serem utilizadas informações pessoais e intimas de uma pessoa jurídica ou física para comercialização.

Embora a Lei Geral de Proteção de Dados, tenha originado no cenário europeu, ao chegar no ordenamento jurídico brasileiro, foi se moldando aos paramentos societários presentes no Brasil.

É uma Lei que proporciona um grande marco normativo no cenário brasileiro, mas ainda assim, há necessidade de se criar resoluções para situações especificas aos acessos digitais.

3 OS IMPACTOS JURÍDICOS DA LGPD NO ORDENAMENTO JURÍDICO BRASILEIRO

O presente capítulo tem por objetivo explanar os princípios norteadores da LGPD como a privacidade e a liberdade, destacando que ambos estão atrelados ao princípio magno da nossa Constituição: a dignidade da pessoa humana. Ademais será explanado também sobre os aparatos normativos que influenciaram na construção da referida Lei em nosso País, como A Declaração Universal dos Direitos do Humanos, Código Civil, Convenção Europeia dos Direitos do Homem, Pacto de São José da Costa Rica bem como, visam apresentar os impactos e principais adaptações necessárias nos relacionamentos entre os indivíduos, sejam eles de forma *on line* ou offline.

3.1 Conceito de Privacidade na Era Digital

A dignidade da pessoa humana, é um direito da personalidade que permeia por todo nosso ordenamento jurídico, e decorrente destes outros direitos foram surgindo para assim regular o convívio social de forma justa e igualitária, e dentre esses direitos destaca- se o direito à privacidade.

Ao esboçar discussões referente a privacidade a priori será elencado de forma mediata a liberdade do indivíduo em manter em particular informações a seu respeito, proporcionado ao sujeito um espaço reservado, conforme explana Vieira (2007, p. 20):

> Nesse sentido a privacidade proporciona ao individuo a oportunidade de desvencilhar-se de todas as máscaras que a sociedade lhe impõe, ou seja, confere-lhe um espaço reservado, seguramente inviolável, em que ele pode explorar livremente o seu íntimo, despido do temos de uma reprimendaexterna, para exercer, enfim, o seu direito de autodeterminação.

Salientar discussões relacionada a privacidade, torna-se imprescindível abranger esse direito concomitante a intimidade e a liberdade, visto que ambos se apresentam como face da mesma moeda, tornando-se direitos indivisíveis, ademais o direito à privacidade possui previsão Legal em nossa carta magna e no Código Civil especificamente nos seguintes artigos:

> Art. 5º, X, CF -são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (Constituição Federal de 1988);

> Art. 21, CC. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. (Código Civil).

A privacidade corresponde a informações particulares de cada indivíduo, e deve ser compreendida de forma que cada um tenha o controle de quais informações podem ser compartilhadas ou publicizadas a terceiros.

O direito à privacidade além da proteção amparada pelos aparatos normativos supracitados, ainda temos esse direito expressamente previsto na Declaração Universal dos Direitos Humanos:

> Artigo 12° "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."

Mas as discussões a respeito da privacidade do indivíduo não é uma discussão recente, um grande marco nessa trajetória que contribuiu para o fortalecimento do direito à privacidade, ocorreu em 1890 nos Estados Unidos da América, onde fora publicado um artigo na *Harvard Law Review, Right to privacy.*

> This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.[4] (BRANDEIS, Louis D. WARREN, Samuel D.. 1890, s.p)

Esse texto possibilitou uma reflexão acerca da proteção jurídica dos pensamentos e emoções dos indivíduos, sem a interposição até mesmo do próprio legislador. Esse artigo permitiu algumas discussões a respeito da subjetividade que trata o direito à privacidade, ou seja, permitiu explanar nuances a respeito da individualidade do sujeito e seus próprios pensamentos.

[4] Este desenvolvimento da lei era inevitável. A intensa vida intelectual e emocional, e o aumento das sensações que vieram com o avanço da civilização, deixaram claro para os homens que apenas uma parte da dor, prazer e proveito da vida estava nas coisas físicas. Pensamentos, emoções e sensações exigiam reconhecimento jurídico, e a bela capacidade de crescimento que caracteriza o common law permitia aos juízes a proteção necessária, sem a interposição do legislador.

Com essa discussão em ascensão, surge nesse cenário a Declaração Universal dos Direitos Humanos, já citado anteriormente, onde especificamente no artigo 12 trata do direito à privacidade e inviolabilidade.

Décadas seguintes, no ano de 1950 surge então A Convenção Europeia dos Direitos do Homem, a qual como resultado originou mais um documento internacional, e que dentro das diversas temáticas, abrangeu o direito e respeito a vida privada, entretanto no âmbito familiar:

> ARTIGO 8°
> Direito ao respeito pela vida privada e familiar
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros. (Carta dos Direitos Fundamentais da EU, 2009, s.p.)

Desde então construções a respeito da referida temática não cessou, cada vez mais o cenário europeu foi investindo em discussões e construções de documentos legislativos que respaldassem a privacidade do indivíduo. Especificamente no ano de 1969, o direito à privacidade conquistou o Artigo 11 da Convenção Americana sobre Direitos Humanos concomitante ao Pacto de São José da Costa Rica. Embora tratassem de documentos que obtivessem um respaldo com previsão em tratados internacionais e de direito humanos o direito à privacidade foi incorporando os ordenamentos jurídicos de cada país, de forma gradativa

Foi a partir da produção desses documentos que os países começaram a se organizar e incorporar em seus ordenamentos jurídicos a penalidade para aqueles que praticassem a violabilidade da privacidade de um indivíduo, a priori sendo discutido no âmbito penal, e depois acontecendo a inclusão dessa discussão na esfera civil.

O primeiro exemplo de pais que inseriu em seu ordenamento jurídico a punição na esfera penal, aqueles que praticassem a violabilidade da privacidade, foi na Alemanha (1967), seguido da Itália (1974).

Observa-se que os exemplos de países exteriores possibilitaram de forma assídua o fomento da temática a respeito da privacidade, sendo incorporado gradativamente em cada ordenamento interno, independente de ratificação com os tratados.

Discutir em um tópico o direito à privacidade, não é algo simples, esse direito possui diversas características relevantes, dentre elas: trata-se de um direito personalíssimo, concedidos a todos e adquiridos no ato do nascimento, vitalícios tendo eficácia muitas vezes *post mortem*, imprescritíveis, irrenunciáveis, dentre outras características.

Mas pra compreendermos a totalidade da relevância do referido princípio, é importante salientar que as dimensões desse princípio, permeiam outros diversos marcos na história da construção dos direitos fundamentais, a qual para seu embasamento possui outros diversos princípios, que será elaborado no próximo item.

3.2 Princípios Aplicáveis

No sentido de possibilitar reflexões a respeito da privacidade, enquanto um pilar do princípio magno de nossa Carta Constitucional, o princípio da dignidade da pessoa humana, torna-se necessário abordar documentos legislativos que contribuíram para a formação dos nossos princípios, como a Carta Europeia.

A Carta Europeia foi adoptada, no ano 2000 apenas como um compromisso político, mas as temáticas abordadas atingiram tamanha relevância mundial que no ano de 2009 a Carta Europeia passou a ter força normativa.

O referido documento, foi elaborado partindo das premissas de liberdade, segurança e justiça, tendo um olhar mais atento as pessoas que seriam e são diretamente impactadas com o conteúdo, em especial a população europeia.

Embora o conteúdo completo do referido documento obtenha tamanha relevância, o principio a ser discorrido nesse item, corresponde diretamente ao objeto da referida pesquisa, ou seja, a privacidade do indivíduo, privacidade essa com previsão no Artigo 8º Carta:

> 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. (Carta dos Direitos Fundamentais da EU, 2009, s.p.)

O distinto artigo esboça claramente a vedação de fornecimento de informações de caráter pessoal sem o devido tratamento, ou seja, sem a devida autorização por parte do indivíduo, possibilitando uma circulação de dados no âmbito europeu de forma desenfreada e sem o devido tratamento legal. Dentre os principais documentos, que a referida carta impactou, destaca-se à DIRETIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO 95/46/CE:

> 2) Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos;
> 4) Considerando que o recurso ao tratamento de dados pessoais nos diversos domínios das actividades económicas e sociais é cada vez mais frequente na Comunidade; que o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados;
> 41) Considerando que todas as pessoas devem poder beneficiar do direito de acesso aos dados que lhes dizem respeito e que estão em fase de tratamento, a fim de
> assegurarem, nomeadamente, a sua exactidão e a licitude do tratamento; que, pelas mesmas razões, todas as pessoas devem, além disso, ter o direito de conhecer a lógica subjacente ao tratamento automatizado dos dados que lhe dizem respeito, pelo menos no caso das decisões automatizadas referidas no nº 1 do artigo 15º; que este último
> direito não deve prejudicar o segredo comercial nem a propriedade intelectual, nomeadamente o direito de autor que protege o suporte lógico; que tal, todavia, não poderá traduzir-se pela recusa de qualquer informação à pessoa em causa

No decorrer da Diretiva existem diversas outras considerações que discorre sobre a proteção de dados com ênfase no direito a privacidade enquanto um direito personalíssimo do indivíduo, estabelecendo assim uma regulação no que diz respeito aos limites da livre circulação de dados pessoais da união europeia.

O interessante em destacar no que fiz respeito aos dois documentos supracitados:

> As regras de proteção de dados são aplicáveis não só quando o tratamento estiver estabelecido no território da União Europeia, mas sempre que o controlador utiliza equipamento situado na UE, a fim de processar dados. Desse modo, os casos referentes ao Facebook (e diversas outras redes sociais) levariam a aplicação da Diretiva 95/46/CE. (HIRATA, 2017, p.)

Ou seja, ainda que existem países que não tenham ratificados os tratados que possuem como base a Carta da União Europeia, ainda assim, para manterem relações no território europeu, tem que respeitar o que prevê o referido documento, em especial no que diz respeito a proteção de dados e o direito a privacidade.

A Carta da União Europeia possui princípios básicos que regem seu fundamento, e em síntese destacam-se os 5 (cinco) princípios éticos para o uso da inteligência artificial, e que por analogia estende-se a proteção de dados. Esses princípios são utilizados especificamente em sistemas judiciais com a finalidade de orientar os legisladores no processo de elaboração de políticas públicas voltadas para o uso da tecnologia de forma segura, visto que os avanços tecnológicos sem duvidas devem adentrar a sociedade contemporânea, contudo sempre respeitando os direitos individuais.

Diante da citação dos princípios basilares que compõem a Carta Europeia, se faz necessário explanar brevemente sobre cada princípio, sendo eles:

> 1. Principle of respect for fundamental rights: ensure that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights The processing of judicial decisions and data must serve clear purposes, in full compliance with the fundamental rights guaranteed by the European Convention on Human Rights (ECHR) and the Convention on the Protection of Personal Data (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 as amended by the CETS amending protocol No. 223). When artificial intelligence tools are used to resolve a dispute or as a tool to assist in judicial decision-making or to give guidance to the public, it is essential to ensure that they do not undermine the guarantees of the right of access to the judge and the right to a fair trial (equality of arms and respect for the adversarial process).They should also be used with due respect for the principles of the rule of lawand judges' independence in their decision-making process. Preference should therefore be given to ethical-by-design2 or humanrights-by-design approaches. This means that right from the design and learning phases, rules prohibiting direct or indirect violations of the fundamental values protected by the conventions are fully integrated[5] (EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), 2018, p.06.)

O distinto princípio explana sobre a necessidade e a importância de as decisões judiciais respeitarem os direitos fundamentais, ainda que estes estejam embasados no desenvolvimento da inteligência artificial. Ocorre que os softwares são maquinas que não

[5] 1. Princípio do respeito pelos direitos fundamentais: garantir que a conceção e implementação de ferramentas e serviços de inteligência artificial sejam compatíveis com os direitos fundamentais sobre os Direitos Humanos (CEDH) e a Convenção sobre a Protecção de Dados Pessoais (Convenção para a Protecção de Indivíduos no que diz respeito ao Processamento Automático de Dados Pessoais, ETS nº 108, conforme alterado pelo protocolo de alteração CETS nº 223). Quando as ferramentas de inteligência artificial são utilizadas para resolver um litígio ou como ferramenta para auxiliar na tomada de decisões judiciais ou para orientar o público, é essencial garantir que elas não prejudiquem as garantias do direito de acesso ao juiz e o direito a um julgamento justo (igualdade de armas e respeito pelo processo contraditório). Devem também ser utilizados com o devido respeito pelos princípios do Estado de direito e pela independência dos juízes no seu processo decisório. Portanto, deve-se dar preferência a abordagens éticas por design2 ou direitos humanos por design. Isso significa que desde as fases de projeto e aprendizado, as regras que proíbem violações diretas ou indiretas dos valores fundamentais protegidos pelas convenções estão totalmente integradas

possuem inteligência autônoma, logo não possuem sentimentos, desta forma o respeito e a valoração aos direitos fundamentais individuais, advém dos indivíduos que elaboram e alimentam esses softwares.

> 2. Principle of non-discrimination: specifically prevent the development or intensification of any discrimination between individuals or groups of individuals: Given the ability of these processing methods to reveal existing discrimination, through grouping or classifying data relating to individuals or groups of individuals, public and private stakeholders must ensure that the methods do not reproduce or aggravate such discrimination and that they do not lead to deterministic analyses or uses. Particular care must be taken in both the development and deployment phases, especially when the processing is directly or indirectly based on "sensitive" data. This could include alleged racial or ethnic origin, socio-economic background, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health-related data or data concerning sexual life or sexual orientation. When such discrimination has been identified, consideration must be given to corrective measures to limit or, if possible, neutralise these risks and as well as to awareness-raising among stakeholders. However, the use of machine learning and multidisciplinary scientific analyses to combat such discrimination should be encouraged.[6] (EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), 2018, p.09.)

O Principio da não discriminação, veda qualquer tipo de discriminação em especial que tenha como base dados informacionais no âmbito da tecnologia utilizando como ferramenta para essa prática a inteligência artificial, em especial quando se tratar de dados caracterizados como "sensíveis", que incluem informações relacionadas a gênero, religião, raça, opiniões politicas e etc. Se por ventura acontecer alguma forma de discriminação, de imediato deve ser impetrado alguma medida que neutralize tal discriminação.

> 3. Principle of quality and security: with regard to the processing of judicial decisions and data, use certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment Designers of machine learning models should be able to draw

1. [6] Princípio da não discriminação: especificamente prevenir o desenvolvimento ou intensificação de qualquer discriminação entre indivíduos ou grupos de indivíduos: Dada a capacidade desses métodos de processamento de revelar a discriminação existente, por meio do agrupamento ou classificação de dados relativos a indivíduos ou grupos de indivíduos, públicos e privados as partes interessadas devem garantir que os métodos não reproduzam ou agravem tal discriminação e que não levem a análises ou usos determinísticos. Deve-se ter um cuidado especial nas fases de desenvolvimento e implantação, especialmente quando o processamento é baseado direta ou indiretamente em dados "sensíveis". Isso pode incluir alegada origem racial ou étnica, antecedentes socioeconômicos, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relacionados à saúde ou dados relativos à vida sexual ou orientação sexual. Quando tal discriminação for identificada, devem ser consideradas medidas corretivas para limitar ou, se possível, neutralizar esses riscos e também a conscientização das partes interessadas. No entanto, o uso de aprendizado de máquina e análises científicas multidisciplinares para combater essa discriminação deve ser incentivado.

> widely on the expertise of the relevant justice system professionals (judges, prosecutors, lawyers, etc.) and researchers/lecturers in the fields of law and social sciences (for example, economists, sociologists and philosophers). Forming mixed project teams in short design cycles to produce functional models is one of the organisational methods making it possible to capitalise on this multidisciplinary approach. Existing ethical safeguards should be constantly shared by these project teams and enhanced using feedback. Data based on judicial decisions that is entered into a software which implements a machine learning algorithm should come from certified sources and should not be modified until they have actually been used by the learning mechanism. The whole process must therefore be traceable to ensure that no modification has occurred to alter the content or meaning of the decision being processed. The models and algorithms created must also be able to be stored and executed in secure environments, so as to ensure system integrity and intangibility.[7]. (EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), 2018, p.10.)

O terceiro princípio aborda a qualidade e segurança em relação as decisões judicias com base em dados, ou seja, se uma decisão judicial for embasada em informações e dados tecnológicos é importante que sejam fontes seguras pautados em critérios éticos proporcionando assim a materialidade da segurança jurídica no âmbito virtual, e conforme coloca Marcato (2022, p. 120):

> Aqui, portanto, é possível fazer uma correlação com o princípio da segurança jurídica. A segurança jurídica é o princípio pelo qual se obriga o Estado a garantir ao seu cidadão que não haverá arbitrariedades na prestação jurisdicional e que as decisões que se derivarem serão justas e isonômicas. Dessa forma, mesmo tendo o Estado o monopólio da jurisdição, mesmo sendo o detentor da última palavra, o que é garantido na própria Constituição Federal, haverá limites a serem observados. Essa atuação sofre, sim, um controle. De maneira geral, a segurança jurídica visa a certeza e a previsibilidade, relacionando-se com valores objetivos atinentes à estabilidade jurídica, que, por via reflexa, gera a confiança na prestação jurisdicional. Tudo isso é possibilitado por um sistema jurídico positivado e uma coerência no sistema de precedentes, com o objetivo último de que a decisão judicial, fruto da prestação jurisdicional, seja necessariamente racional, coerente e controlável.

[7] 3. Princípio da qualidade e segurança: no que diz respeito ao processamento de decisões judiciais e dados, utilizar fontes certificadas e dados intangíveis com modelos concebidos de forma multidisciplinar, em ambiente tecnológico seguro. amplamente na experiência dos profissionais relevantes do sistema de justiça (juízes, promotores, advogados, etc.) e pesquisadores/docentes nas áreas de direito e ciências sociais (por exemplo, economistas, sociólogos e filósofos). A formação de equipes de projeto mistas em ciclos de projeto curtos para produzir modelos funcionais é um dos métodos organizacionais que permitem capitalizar essa abordagem multidisciplinar. As salvaguardas éticas existentes devem ser constantemente compartilhadas por essas equipes de projeto e aprimoradas por meio de feedback. Os dados baseados em decisões judiciais que são inseridos em um software que implementa um algoritmo de aprendizado de máquina devem vir de fontes certificadas e não devem ser modificados até que sejam realmente usados pelo mecanismo de aprendizado. Todo o processo deve, portanto, ser rastreável para garantir que nenhuma modificação tenha ocorrido para alterar o conteúdo ou o significado da decisão que está sendo processada. Os modelos e algoritmos criados devem também poder ser armazenados e executados em ambientes seguros, de forma a garantir a integridade e intangibilidade do sistema. Princípio da transparência, imparcialidade e equidade

A segurança jurídica dever ser seguida no âmbito dos processos físicos, e tal princípio não difere no que diz respeito aos processos virtuais, ou seja, torna-se imprescindível a garantia da segurança jurídica também no âmbito virtual, seja em relação as decisões ou até o armazenamento dessas.

> 4. Principle of transparency, impartiality and fairness: make data processing methods accessible and understandable, authorise external audits A balance must be struck3 between the intellectual property of certain processing methods and the need for transparency (access to the design process), impartiality (absence of bias)4 , fairness and intellectual integrity (prioritising the interests of justice) when tools are used that may have legal consequences or may significantly affect people's lives. It should be made clear that these measures apply to the whole design and operating chain as the selection process and the quality and organisation of data directly influence the learningphase. The first option is complete technical transparency (for example, open source code and documentation), which is sometimes restricted by the protection of trade secrets. The system could also be explained in clear and familiar language (to describe how results are produced) by communicating, for example, the nature of the services offered, the tools that have been developed, performance and the risks of error. Independent authorities or experts could be tasked with certifying and auditing processing methods or providing advice beforehand. Public authorities could grant certification, to be regularly reviewed.[8] EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), 2018, p.11.)

O quarto princípio, discorre sobre o Princípio da Transparência, imparcialidade e justiça, e no que diz respeito ao âmbito do poder judiciário o mesmo, assim como os demais órgãos do poder público devem seguir tal princípio em sua integralidade, ainda que esteja no âmbito da transparência tecnológica. Contudo ainda que esse princípio preconize a garantia de dados acessíveis, é importante destacar que existem dados individuais de caráter sigiloso por isso a necessidade de compreensão no equilíbrio entre

[8] 4. Princípio da transparência, imparcialidade e justiça: tornar os métodos de processamento de dados acessíveis e compreensíveis, autorizar auditorias externas Deve-se encontrar um equilíbrio entre a propriedade intelectual de certos métodos de processamento e a necessidade de transparência (acesso ao processo de design), imparcialidade (ausência de parcialidade), justiça e integridade intelectual (priorizando os interesses da justiça) quando são utilizadas ferramentas que podem ter consequências legais ou podem afetar significativamente a vida das pessoas. Deve ficar claro que essas medidas se aplicam a toda a cadeia de projeto e operação, pois o processo de seleção e a qualidade e organização dos dados influenciam diretamente na fase de aprendizado. A primeira opção é a transparência técnica completa (por exemplo, código-fonte aberto e documentação), que às vezes é restringida pela proteção de segredos comerciais. O sistema também pode ser explicado em linguagem clara e familiar (para descrever como os resultados são produzidos), comunicando, por exemplo, a natureza dos serviços oferecidos, as ferramentas que foram desenvolvidas, o desempenho e os riscos de erro. Autoridades independentes ou especialistas podem ser encarregados de certificar e auditar métodos de processamento ou fornecer aconselhamento prévio. As autoridades públicas poderiam conceder a certificação, a ser revisada regularmente.

dados tecnológicos e o princípio da transparência, em especial em dados que podem impactar diretamente a vida das pessoas.

> 5. Principle "under user control": preclude a prescriptive approach and ensure that users are informed actors and in control of their choices User autonomy must be increased and not restricted through the use of artificial intelligence tools and services. Professionals in the justice system should, at any moment, be able to review judicial decisions and the data used to produce a result and continue not to be necessarily bound by it in the light of the specific features of that particular case. The user must be informed in clear and understandable language whether or not the solutions offered by the artificial intelligence tools are binding, of the different options available, and that s/he has the right to legal advice and the right to access a court. S/he must also be clearly informed of any prior processing of a case by artificial intelligence before or during a judicial process and have the right to object, so that his/her case can be heard directly by a court within the meaning of Article 6 of the ECHR. Generally speaking, when any artificial intelligence-based information system is implemented there should be computer literacy programmes for users and debates involving professionals from the justice system.[9] EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), 2018, p.12.)

Por fim, o quinto principio da Carta Europeia aborda o Principio de Controle do Usuário, ou seja, se trata de um mecanismo executado pela inteligência artificial que ao acessar determinados conteúdos na internet, os dados do navegante ficaram retidos naquela plataforma, nessas hipóteses o usuário navegante precisa ter ciência do feito, bem como, existem casos em que ensejam a autorização expressa para tal coleta.

Esboçar os princípios que regem o direito a privacidade, possibilita uma compreensão da amplitude que esse direito possui, visto que sua construção ocorre em escala mundial, onde a LGPD promulgada em território brasileiro, não surgiu de uma simples ideia dos legisladores, mas de construções históricas pelo mundo todo, que como citado anteriormente atingiu de forma mais impactante a união europeia e demais países que possuem relações com a mesma, além dos EUA e Itália.

[9] 5. Princípio "sob controle do usuário": impedir uma abordagem prescritiva e garantir que os usuários sejam atores informados e no controle de suas escolhas A autonomia do usuário deve ser aumentada e não restringida pelo uso de ferramentas e serviços de inteligência artificial. Os profissionais do sistema de justiça devem, a qualquer momento, poder rever as decisões judiciais e os dados utilizados para produzir um resultado e continuar não necessariamente vinculados a ele à luz das características específicas daquele caso concreto. O usuário deve ser informado em linguagem clara e compreensível se as soluções oferecidas pelas ferramentas de inteligência artificial são vinculantes ou não, das diferentes opções disponíveis, e que tem direito a aconselhamento jurídico e direito de acesso a um tribunal. Deve também ser claramente informado de qualquer processamento prévio de um caso por inteligência artificial antes ou durante um processo judicial e ter o direito de se opor, para que o seu caso possa ser ouvido diretamente por um tribunal na aceção do artigo 6.º da CEDH. De modo geral, quando qualquer sistema de informação baseado em inteligência artificial for implementado, deve haver programas de alfabetização computacional para os usuários e debates envolvendo profissionais do sistema de justiça.

Salientar sobre os princípios norteadores do direito a privacidade, é uma forma introdutória para demonstrar que esse direito embora tenha obtido maior relevância com a chegada eficaz de aparatos normativos que o regem na sociedade contemporânea, ainda assim possui uma construção mundial e abrange diversos países.

Sendo assim, no próximo item será discorrido sobre a relação desse direito no que diz respeito a violação do mesmo, por meio do mecanismo de comercialização de dados.

3.3 Proteção de Dados *Versus* Comercialização de Dados

A relevância e importância em relação aos dados pessoais, tornaram-se o novo petróleo do século XXI em decorrência da valorização do mesmo. A produção de informações com esses dados, ganharam um reforço com a expansão da internet, em que a mesma conta com mecanismos de:

> [...] busca que catalogam os sites e realizam pesquisa na rede, a partir de uma palavra-chave fornecida pelo usuário. Representa uma tendência de produção de informação nas mãos de grandes grupos de comunicação, contribui para a pluralização da produção de informações dando, potencialmente, a grupos menores e a indivíduos isolados as mesmas condições técnicas de produzir mensagens e atingir o mesmo público potencial. Com o crescimento súbito da internet, ocorre uma grande proliferação de sites, chats, redes sociais — orkut, facebook, msn, twitter —, tornando a internet uma rede ou teia global de computadores conectados aproximando pessoas, culturas, mundos e informações. Hoje em dia, a Internet é utilizada mundialmente como ferramenta de trabalho, diversão, comunicação, educação, informação. Saiu-se de um mundo físico e criou-se um mundo "paralelo" em que permanecemos conectados o tempo todo. (PRATES, 2021, s.p.)

Ou seja, a internet possibilita uma conexão de pessoas e informações de maneira simultânea e em um curto espaço de tempo, e mais, cada acesso deixa um rastro nas mídias tecnológicas, também conhecido tecnicamente como um histórico de busca e pesquisas, que juntos formam um conjunto de informações, composto inclusive por dados pessoais.

O monitoramento e o controle dessa rede, é quasse impossível de ser realizada, por suas características subjetivas, e em decorrência de que seu avanço não correspondeu com os avanços de controle da sociedade contemporânea.

Esse avanço do mundo digital no âmbito da internet, trouxe grandes preocupações para o ordenamento jurídico brasileiro, visto que as normativas não se encontravam aptas para proteção integral dos usuários desses sistemas e da era digital, em especial no que diz respeito aos dados pessoais.

Diante dessa instabilidade na segurança jurídica, surgiram lacunas no percurso de armazenamento de informações no âmbito da internet, proporcionando assim um vazamento de dados pessoais de forma desenfreada, conforme aponta notícias do CNN Brasil:

> Quatro em cada dez empresas sediadas no Brasil tomam medidas protetivas contra o vazamento de dados sigilosos e pessoais dos clientes, mostra uma pesquisa elaborada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic).
> A análise foi feita com base na resposta de mais de 4 mil empresários, coletadas entre agosto de 2021 e abril de 2022.
> As ações contra o vazamento de informações sensíveis cresceram 42% nos últimos dois anos, desde o início da pandemia de Covid-19, mostra o levantamento, que fala em quase três milhões de ataques hackers no Brasil durante o primeiro semestre de 2022 – alta de quase 10% em relação os primeiros seis meses de 2021.
> Especialistas do Cetic apontam que as interações online tiveram um "boom" desde o início da crise sanitária, facilitando a divulgação indevida de dados sigilosos. (CNN Brasil, 2022, s.p.)

Como uma tentativa de minimizar esses danos, surgiu então a promulgação da LGPD, conforme já abordado no capítulo anterior, tem como principal objetivo realizar o tratamento de dados pessoais, com ênfase nos meios digitais, visando garantir a proteção dos direitos fundamentais de liberdade e de privacidade.

A proteção integral dos cidadãos, não é algo recente, em especial no que diz respeito a liberdade, desde que essa liberdade não ocasione lesão a liberdade de terceiros, como bem coloca Warren e Brandeis (2016, p. 6):

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.[10]

[10] Que o indivíduo tenha plena proteção pessoal e patrimonial é um princípio tão antigo quanto a lei comum; mas foi considerado necessário, de tempos em tempos, definir novamente a natureza exata e a extensão de tal proteção. As mudanças políticas, sociais e econômicas implicam o reconhecimento de novosdireitos, e o direito comum, em sua eterna juventude, cresce para atender às novas demandas da sociedade.

Ou seja, embora a proteção integral dos indivíduos seja um direito antigo, ainda assim precisa estar em constante revisão, para assim atender as demandas da sociedade contemporânea, e de fato, a proteção de dados na esfera digital materializa essa informação, e o avanço das normativas jurídicas tornou-se inevitável.

Ocorre que quando falamos em comercialização de dados, em proteção integral e etc, empiricamente e de forma imediata entendemos que essa comercialização advém apenas das multinacionais, de grandes empresas, ou seja, apenas de setores privados, mas nos esquecemos que a desproteção e a violação também podem tendenciar a advir daqueles órgãos que deveriam proteger.

Um exemplo de situação como essa foi a que ocorreu em Reading na Pensilvânia, localizada especificamente a 80 (oitenta) quilômetros da Filadelfia, onde nessa pequena região ocorreu um declínio na economia o que impactou drasticamente na pobreza. Com todo esse declínio na economia, a arrecadação de impostos também sofreu impactos, o que ocasionou em uma demissão em massa, atingindo inclusive no desligamento de policiais da região, ocorrendo 45 (quarenta e cinco) demissões de policiais:

> The small town of Reading, Pennsylvania, experienced a difficult in the post-industrial era. Nestled in the green hills fifty miles west of Philadelphia, Reading grew rich from railroads, steel, coal and textiles. But in the last decades, with all these industries in sharp decline, the city languished. In 2011, it had the highest poverty rate in the country, at 41.3%. (The following year, it was surpassed, if barely, by Detroit.) As recession hit Reading's economy after the crash of the 2008 market, tax revenues fell, which led to a cut of 45 police officers in the police department – despite persistent crime.[11] (NEIL, 2016, p. 76).

Diante da situação, o responsável pelo policiamento da região, pensou em estratégias para que mantivesse o efetivo policiamento, mas agora com 45 (quarenta e cinco) policiais a menos. Sendo assim, o referido policial investiu em um software que tinha como principal objetivo e função prever crimes, ou seja, tratava-se de um programa que processava dados históricos de crimes calculando assim hora e data onde poderia haver maior probabilidade que os crimes acontecessem.

[11] A pequena cidade de Reading, na Pensilvânia, passou por uma situação difícil na era pós-industrial. Aninhado nas colinas verdes a oitenta quilômetros a oeste da Filadélfia, Reading enriqueceu com ferrovias, aço, carvão e têxteis. Mas nas últimas décadas, com todas essas indústrias em declínio acentuado, a cidade definhou. Em 2011, tinha a maior taxa de pobreza do país, com 41,3%. (No ano seguinte, foi superado, se mal, por Detroit.) À medida que a recessão atingiu a economia de Reading após o crash do mercado de 2008, as receitas fiscais caíram, o que levou a um corte de 45 policiais no departamento de polícia – apesar do crime persistente. NEIL, 2016, p. 76)

> O program processed historical crime data and calculated, hour by hour, where crimes were most likely to occur. Reading officers could see the program's findings as a series of squares, each the size of two football fields. if they spent more spent patrolling these squares, there was a good chance of deterring crime. Predictive programs like PredPol are all the rage in police departments with limited budget across the country. Departments from Atlanta to Los Angeles are mobilizing police in the moving squares and reporting the drop in crime rates. New York City uses a similar program called CompStat. and the police Philadelphia is using a local product called HunchLab that includes terrain analysis of risk, which incorporates certain features, such as ATMs or convenience stores, that may attract crimes. As in the rest of the Big Data industry, software developers of crime forecasters are racing to incorporate any information that might increase the accuracy of your models. Predictive crime models like PredPol have their virtues. Unlike the criminals in the movie Steven Spielberg's dystopian Minority Report (and some sinister real-life initiatives, which we'll see soon), police officers don't track people down before they commit crimes. Jeffrey Brantingham, the UCLA professor of anthropology who founded PredPol, emphasized to me that the model is blind to race and ethnicity. AND badly, for Detroit.) As recession hit Reading's economy after the crash of 2008 market, tax revenues fell, which led to a cut of 45 police officers in the police department – despite persistent crime. And sure enough, a year later, Chief Heim announced that robberies were down 23%.[12](NEIL, 2016, p. 76)

O Programa PredPol, utilizado para auxiliar no policiamento, obteve um resultado positivo e considerável visto que, conforme apresenta-se na citação acima, a quantidade de roubos caiu 23%. Com esses resultados positivos, a quantidade de cidades que investiram na implantação de software semelhantes, que contribuíssem no policiamento, e assim reduzissem os índices de criminalidades, além posicionar os policiais onde os crimes pareciam ser mais prováveis de acontecer, gerando assim a otimização de custos.

[12] O programa processava dados históricos de crimes e calculava, hora a hora, onde os crimes eram mais prováveis de ocorrer. Os policiais de Reading podiam ver as conclusões do programa como uma série de quadrados, cada um do tamanho de dois campos de futebol. Se passassem mais tempo patrulhando essas praças, havia uma boa chance de desencorajar o crime. Programas preditivos como o PredPol estão na moda em departamentos de polícia com orçamento limitado em todo o país. Departamentos de Atlanta a Los Angeles estão mobilizando policiais nas praças em movimento e relatando a queda das taxas de criminalidade. A cidade de Nova York usa um programa semelhante, chamado CompStat. E a polícia da Filadélfia está usando um produto local chamado HunchLab que inclui análise de terreno de risco, que incorpora certos recursos, como caixas eletrônicos ou lojas de conveniência, que podem atrair crimes. Assim como no restante da indústria de Big Data, os desenvolvedores de software de previsão de crimes estão correndo para incorporar qualquer informação que possa aumentar a precisão de seus modelos. Modelos de crime preditivo como o PredPol têm suas virtudes. Ao contrário dos criminosos no filme distópico de Steven Spielberg Minority Report (e algumas iniciativas sinistras da vida real , que veremos em breve), os policiais não rastreiam as pessoas antes de cometerem crimes. Jeffrey Brantingham, o professor de antropologia da UCLA que fundou a PredPol, enfatizou para mim que o modelo é cego para raça e etnia. E mal, por Detroit.) À medida que a recessão atingiu a economia de Reading após o crash do mercado de 2008, as receitas fiscais caíram, o que levou a um corte de 45 policiais no departamento de polícia – apesar do crime persistente. E com certeza, um ano depois, o chefe Heim anunciou que os roubos caíram 23%. - NEIL, 2016, p. 7)

A princípio, foi um excelente investimento, mas não obteve apenas bônus, com o passar do tempo foi surgindo os ônus desse o investimento, enquanto o Programa PredPol implantado na cidade de Reading produzia apenas dados geográficos, outros softwares começaram a ser utilizados até mesmo como diretrizes para condenação, além do sistema começar a identificar condutas não criminosas ou de baixo potencial ofensivo ocorrendo assim:

> These pesky crimes are endemic in many poor neighborhoods. In some places the police calls them antisocial behavior, or ASB. Unfortunately, including them in the threat model distort the analysis. Once the nuisance data flows into a predictive model, more Police officers are drawn to these neighborhoods, where they are more likely to arrest more people. After all, even if their goal is to stop robberies, murders and rapes, they are doomed. to have slow menstrual periods. It's the nature of patrolling. And if a patrol officer sees a couple of boys who don't look like they're over sixteen drinking from a bottle in a brown bag, he stops them. These types of low-level crimes fill their modelswith more and more points, and the models send the cops back to the same neighborhood.[13] (NEIL, 2016, p.78).

Com essa produção de informações dentro do sistema, começaram a ocorrer diversas prisões com pessoas consideradas culpadas de crimes sem vítimas, com resultados de prisões de pessoas negras e residentes em bairros pobres. Ainda que o sistema não tenha esse entendimento de segregação, foi acontecendo exatamente isso, uma política de tolerância zero para crimes de menor potencial ofensivo ou ate mesmo apenas por condutas antissociais.

Mas crimes como fraudes, crimes envolvendo políticos, infelizmente o PredPol não rastreia, ou seja, a alimentação do sistema é realizada por policiais, que se concentram em registrar situações que acontecessem em regiões periféricas, deixando passar crimes de alto nível ofensivo.

O que era pra ser algo produtivo foi se tornando uma segregação de minorias perseguidas pelo sistema judiciário “Black men, they argued, were six times more likely to being arrested than white men and 21 times more likely to be killed by the police, less

[13] Esses crimes incômodos são endêmicos em muitos bairros pobres. Em alguns lugares, a polícia os chama de comportamento antissocial, ou ASB. Infelizmente, incluí-los no modelo ameaça distorcer a análise. Uma vez que os dados do incômodo fluem para um modelo preditivo, mais policiais são atraídos para esses bairros, onde é mais provável que eles prendam mais pessoas. Afinal, mesmo que seu objetivo seja impedir assaltos, assassinatos e estupros, eles estão fadados a ter períodos menstruais lentos. É a natureza do patrulhamento. E se um policial de patrulha vê um casal de garotos que não parecem ter mais de dezesseis anos bebendo de uma garrafa em um saco marrom, ele os impede. Esses tipos de crimes de baixo nível preenchem seus modelos com mais e mais pontos, e os modelos enviam os policiais de volta ao mesmo bairro. (NEIL, 2016, p.78)

in line with available data (which is notoriously underreported) formalized in an algorithm"[14]

Não existe a possibilidade de conceituar subjetivamente o significado de justiça, visto que trata-se de um software, onde este realiza suas funções de acordo com as informações fornecidas, ou seja, a utilização desse software era pra ser um mecanismo que contribuísse para minimizar os índices de criminalidade, no entanto o que aconteceu foi uma discriminação algoritmo, onde o software foi sendo alimentado com falsas denúncias, condutas de cunho antissocial e não criminosa, contribuindo assim para praticas de discriminação e abordagens policias totalmente desnecessárias.

Diante disso, uma ferramenta que deveria proteger, na verdade produziu informações discriminatórias, destacando que essas informações em especial produzidas pela ferramenta PredPol possibilitou a criação de mapas de software on line que apontasse os locais de maiores índices de criminalidade ou possíveis criminalidades.

Ocorre que o sistema foi apontando bairros pobres, onde residem pessoas negras os caracterizando automaticamente como pessoas mais propensas aos crimes. Quando fora citado no inicio desse item sobre a desproteção de órgãos que deveriam proteger, o exemplo desse software se enquadra para realizarmos uma analogia no que diz respeito a essa destruição de massa que tem como principal álibi os dados pessoais dos indivíduos.

Diante disso, sob a compreensão do zelo no manuseio de informações, o próximo item será explanado sobre os impactos que a LGPD proporcionou nos negócios jurídicos nessa sociedade moderna, também conhecida como sociedade digital.

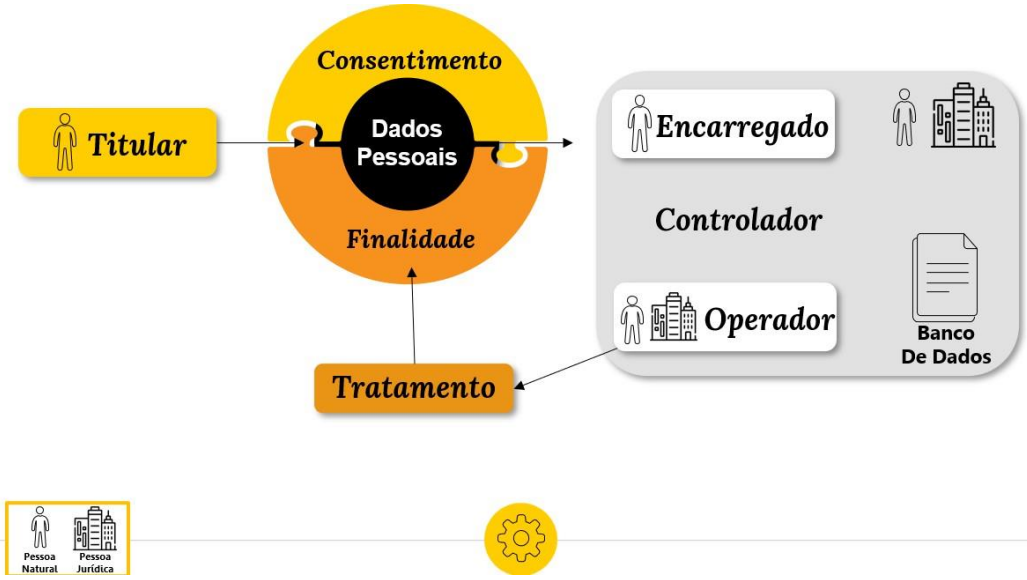
3.4 Os impactos da LGPD nos negócios jurídicos na era digital

Como já mencionado nos itens anteriores, a LGPD foi construída para atender as demandas que a transformação digital proporcionou na sociedade contemporânea, visto que o referido aparato normativo traz consigo uma série de deveres que precisam ser respeitados ao lidar com dados pessoais, visto que a ideia é a proteção integral desses dados, de modo que proporcione a garantia da privacidade, segurança e o direito do indivíduo em fornecer ou não informações a seu respeito. A LGPD então traz consigo novas regras para o uso de dados no Brasil, desde as relações online quanto offline.

[14] Homens negros, eles argumentaram, tinham seis vezes mais chances de serem presos do que homens brancos e 21 vezes mais chances de serem mortos pela polícia, pelo menos de acordo com os dados disponíveis (que são notoriamente subnotificados) formalizado em um algoritmo.

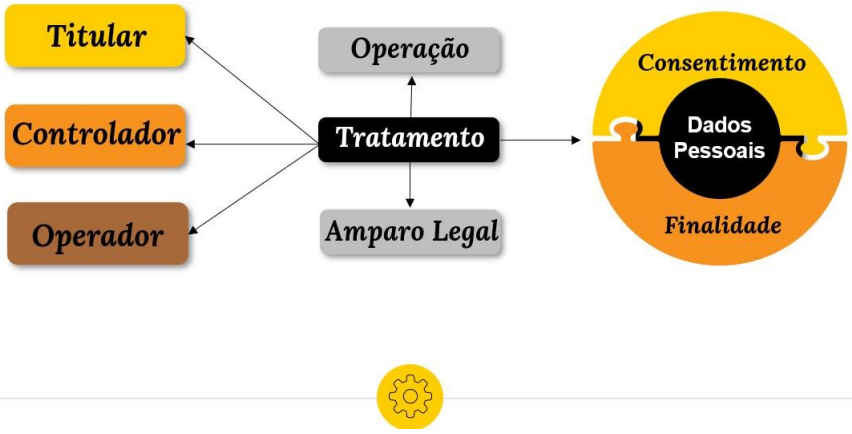
Além das regras de relações no âmbito dos negócios jurídicos, a mesma apresenta também definições de alguns termos como: dado pessoal, tratamento de dados, controlador, operador, autorização para tratamento de dados – e este possui toda uma cronologia a ser seguida:

FIGURA 1 – CRONOLOGIA NO TRATAMENTO DE DADOS



Fonte: elaborado pela autora através da ferramenta powerpoint.

FIGURA 2 - TRATAMENTO DE DADOS



Fonte: elaborado pela autora através da ferramenta powerpoint.

A figura 2 apresenta o que esboça o artigo 41 da LGPD, no que diz respeito a ao responsável encarregado pelo tratamento de dados:

> Conforme o artigo 41 da LGPD, deverá ser nomeado um responsável para ser o Encarregado pelo Tratamento de Dados. O Encarregado é a pessoa que atuará como canal de comunicação perante os titulares dos dados pessoais e aos órgãos reguladores. Ele deverá supervisionar todas as práticas de tratamento de dados pessoais dentro da organização e verificar se estas estão em conformidade com a Lei de proteção de dados. O Encarregado é semelhante ao Data Protection Officer (DPO) do Regulamento Geral sobre a Proteção de Dados (GDPR). (Marcelo Dias de Sá, 2019, pag. 20).

Além do manuseio, tratamento, privacidade, consentimento, a LGPD também trouxe em seu texto normativo sanções para aqueles que violarem os deveres previsto na Lei:

> A LGPD prevê sanções para quem não tiver boas práticas. Elas englobam advertência, multa ou até mesmo a proibição total, ou parcial de atividades relacionadas ao tratamento de dados. As multas podem variar de 2% do faturamento do ano anterior até a R$ 50 milhões, passando por penalidades diárias. A Lei também prever a obrigação de divulgação de incidentes, a eliminação de dados pessoais e a inversão de ônus da prova a favor do titular do dado. (SÁ, 2019, p. 21).

A LGPD trouxe para dentro das relações, em especial nos negócios jurídicos pontos a serem readequados, em especial no que diz respeito a politica de privacidade que deve ser mais clara de fácil entendimento do usuário.

A ciência e compreensão sobre como serão realizados os tratamentos de dados, também foi uma exigência contida na normativa e a autorização para tratamento de dados está discorrida no artigo 11 da LGPD.

É importante salientar que essa adaptação não é apenas para as empresas privadas, mas também para o poder público.

Toda essa adaptação com a LGPD, é a reafirmação que o direito fundamental de privacidade alinhado com a proteção deve ser garantido independente dos avanços da sociedade informacional.

4 LGPD E A APLICAÇÃO PELOS TRIBUNAIS BRASILEIROS- ANÁLISE DE JURISPRUDÊNCIA

O referido capitulo, tem por objetivo apresentar a materialidade da Lei Geral de Proteção de Dados, nos tribunais brasileiros, ressaltando que desde sua promulgação a mesma tem proporcionado grandes discussões nos referidos tribunais para a implementação de ações que garanta a efetividade e o cumprimento do que prevê o distinto aparato normativo.

A Lei Geral de Proteção de dados, possibilitou grandes transformações no ordenamento jurídico brasileiro, em especial na esfera das relações que envolvam os dados pessoais, em síntese a LGPD proporcionou modernidade no mundo jurídico.

Como discorrido nos capítulos anteriores, a LGPD não se trata de uma normativo complementar a outras normativas, como por exemplo o Código Civil ou o Código de Defesa do Consumidor, a LGPD possui status normativos autônomos, que se explorada de forma precisa, proporciona um exponencial de discussões e fundamentações jurídicas.

A dimensão de tal normativa é tamanha, que a mesma adentrou o ordenamento jurídico brasileiro no ano de 2018 (dois mil e dezoito), contudo entrou em vigência somente no ano de 2020 (dois mil e vinte) e as questões punitivas começaram a vigorar apenas em agosto de 2021 (dois mil e vinte e um), ou seja, a complexidade e o tamanho conteúdo a ser explorado nessa normativa se tornou imensurável, de modo que originou-se a necessidade de adaptação do ordenamento jurídico de aproximadamente três anos desde que a referida lei foi sancionada.

O Conselho Nacional de Justiça – CNJ – entendeu ser necessário a promulgação de uma recomendação que explanasse sobre as medidas de adequação necessárias para adaptação da LGPD:

> Artigo 1º Resolução Nº 363 de 12/01/2021
> Temas: Tecnologia Da Informação E Comunicação; Gestão da Informação e de Demandas Judiciais; Gestão e Organização Judiciária; Transparência;
> Ementa: Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.
> Art. 1º Estabelecer medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) a serem adotadas pelos tribunais do país (primeira e segunda instâncias e Cortes Superiores), à exceção do Supremo Tribunal Federal, para facilitar o processo de implementação no âmbito do sistema judicial[...]

Além da referida Resolução, fora criado pelo Superior Tribunal de Justiça (STJ) a Portaria STJ/GDG N. 178 DE 12 DE MARÇO DE 2021, que institui o Comitê Gestor de Proteção de Dados Pessoais (CGPD). Tal comitê teve por função principal implementar a Lei Geral de Proteção de Dado nos tribunais brasileiros.

Dentre as principais ações proporcionadas pelo referido comitê no que diz respeito a educação da LGPD no STJ, destaca-se a implementação da Ouvidoria STJ, como forma de garantir o que prevê o Artigo 18 da LGPD.

Para uma melhor compressão, será explanado uma linha do tempo das principais ações adotadas pelo STJ para garantia de entendimento e implementação da LGPD no ordenamento jurídico brasileiro:

QUADRO 1 – LINHA DO TEMPO DA TRAJETÓRIA DA LGPD NO STJ

Fonte: Imagem elaborada pela autora. Informações extraídas de stj.jus.br

QUADRO 2 – NORMATIVAS E SEUS CONTEÚDOS

NORMATIVAS	O QUE REGULAMENTA
LGPD: Lei Geral de Proteção de Dados Pessoais:	Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Lei 13.853/2019	Criação da figura de Autoridade Nacional de Proteção de Dados.
Lei 14.010/2020	Visa prorrogar a vigência doas artigos da LGPD que tratam de sanções administrativas e multas decorrentes da violabilidade do que prevê a LGPD.
Recomendação nº 73/2020 do Conselho Nacional de Justiça	Recomenda aos órgãos do Poder Judiciário brasileiro a adoção de medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados – LGPD.
Resolução Nº 334	Institui o Comitê Consultivo de Dados Abertos e Proteção de Dados no âmbito do Poder Judiciário.
Portaria nº 213	Institui Comitê Gestor da Lei Geral de Proteção de Dados Pessoais (CGLGPD) no âmbito do Conselho Nacional de Justiça, e dá outras providências.
Portaria nº 212	Institui Grupo de Trabalho destinado à elaboração de estudos e de propostas votadas à adequação dos tribunais à Lei Geral de Proteção de Dados e dá outras providências.

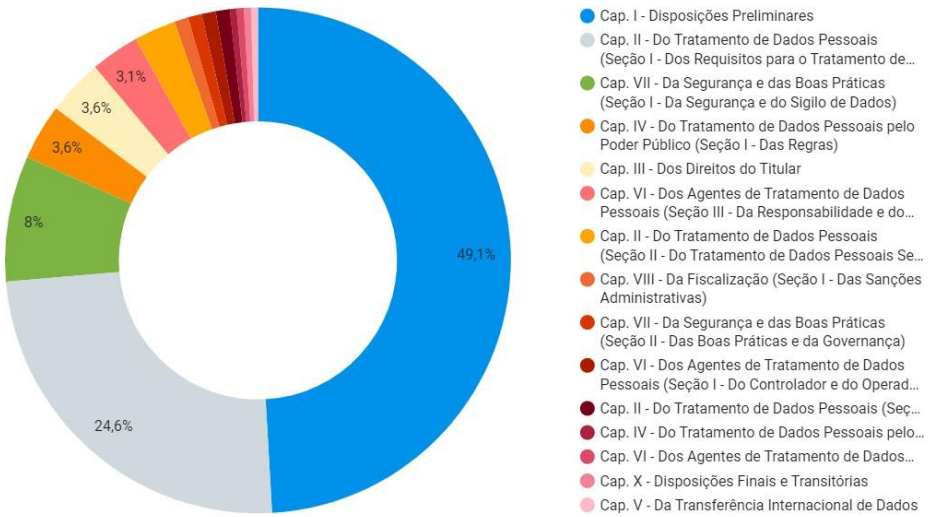
Como bem se observa no decorrer dos capítulos apresentados, e em especial ao distinto capitulo, é possível constatar que com o passar dos anos, houve uma tendencia

em proteger os dados sensíveis do indivíduo, de forma que seja materializado a proteção aos direitos fundamentais, tendencia essa que permeou desde as primeiras leis europeias discutidas nas decidas de 1970 a 1980 (como já citado no capitulo 2) tendo sido impulsionado através da ascensão do avanço da computação e da indústria nos países mais desenvolvidos, a promulgação da Constituição de 1988 no Brasil que em seu artigo 5º já tratava de forma geral sobre a privacidade dos brasileiros.

A partir da promulgação da Constituição de 1988, adentrou ao ordenamento jurídico o Código de Defesa do Consumidor que direcionou a construção de um manual especifico que regulamentava as relações entre empresas e clientes, seguida foi criado a Diretiva 95 da União Europeia que estabeleceu regras a serem cumpridas por toda a união europeia, com ênfase no desenvolvimento de seu texto, em que frisou a proteção de dados pessoais, de forma genérica, em seguida foi possível o Marco Civil da Internet e a grandiosa Lei Geral de Proteção de Dados.

Para compreendermos a relevância da implementação da referida normativa o Centro de Direito, Internet e Sociedade (CEDIS-IDP) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) realizaram em conjunto uma seleção de decisões judiciais que estão marcando a trajetória jurídica da LGPB no ordenamento brasileiro. Essa seleção contou cm uma análise de 584 (quinhentas e oitenta e quatro) decisões, publicadas entre setembro de 2020 e agosto de 2021.

FIGURA 4 – DECISÕES JUDICIAIS COM FUNDAMENTO NA LGPD

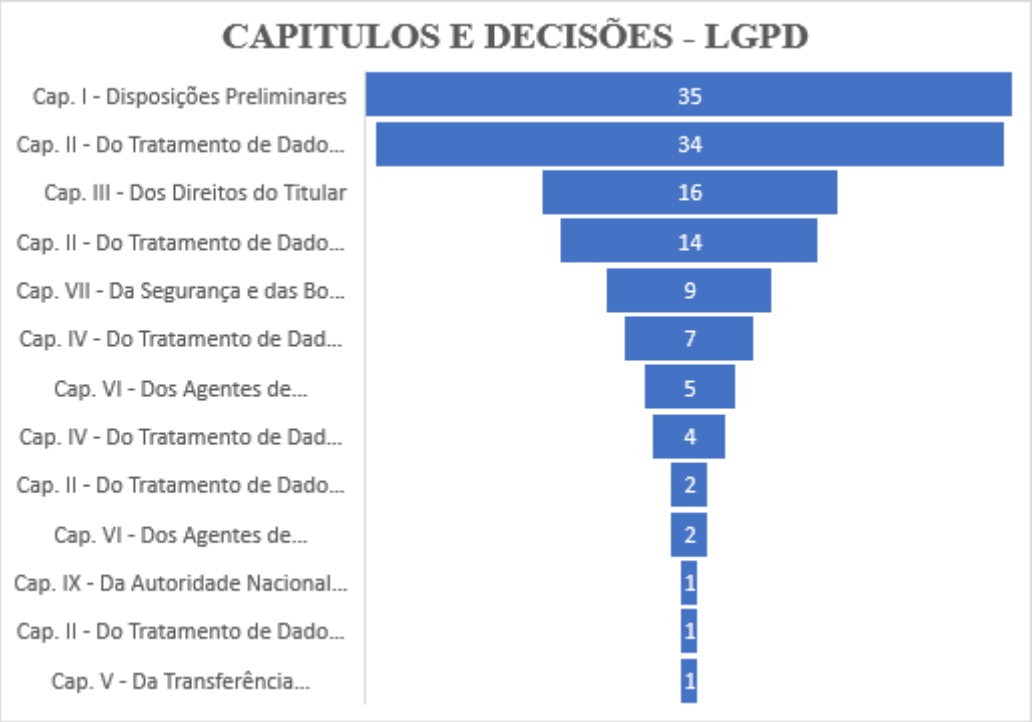


Fonte: Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS-IDP).

Conforme apresenta o gráfico da pesquisa acima, a maioria das decisões analisadas, estão fundamentadas no que prevê o Capitulo 1º da LGPD, com menção aos artigos 2º, 5º e 7º.

Outros indicadores relevantes de serem apresentados, corresponde a quantidade de decisões de acordo com cada capitulo da Lei Geral de Proteção de Dados, ressaltando, que, essa analise corresponde ao universo apresentado de 584 (quinhentas e oitenta e quatro) decisões, publicadas entre setembro de 2020 e agosto de 2021.

FIGURA 5 – RELAÇÃO DAS DECISÕES PROFERIDAS E A FUNDAMENTAÇÃO NA LGPD



Fonte: Gráfico elaborado pela autora, indicadores extraídos do Centro de Direito, Internet e Sociedade do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS-IDP).

À medida que a LGPD se perpetua no ordenamento jurídico brasileiro, adquire-se mais legitimidade proporcionando segurança jurídica em suas decisões, um exemplo dessa afirmativa se consolida com uma decisão em que um Magistrado da 17ª Vara Cível de Brasília, determinou que um site se suspende o anuncio de venda de dados cadastrais, referente ao processo PJe: 0733785-39.2020.8.07.0001:

> O juiz da 17ª Vara Cível de Brasília determinou, em liminar, que o portal Mercado Livre suspenda o anúncio referente a venda de banco de dados e cadastro em geral. Foi determinando ainda que a empresa Sidnei Sassi abstenha-se de disponibilizar, de forma gratuita ou onerosa, digital ou física, dados pessoais de quaisquer indivíduos. A multa é de multa de R$ 2 mil para cada operação. A decisão foi tomada com base na **Lei Geralde Proteção de Dados (LGPD).**
> Autor da ação, o Ministério Público do Distrito Federal e Territórios - MPDFT afirma que foi identificada a comercialização de dados pessoais de brasileiros por meio do site Mercado Livre. Narra que o vendedor, oferta banco de dados e cadastros e que o principal beneficiário é uma empresa do Rio Grande do Sul. O MPDFT argumenta que a **prática ofende a privacidade daqueles cujos dados são comercializados.** (Tribunal de Justiça do Distrito Federal e dos Territórios, 2020, s.p.)

O Magistrado observou na situação, que a empresa realizava a comercialização de dados pessoais, através da plataforma Mercado Livre, sendo no caso especifico a principal beneficiária uma empresa do Rio Grande do Sul.

Para melhor compreensão da lide, se torna necessário apresentar a Ementa:

> APELAÇÃO CÍVEL. DIREITO PROCESSUAL CIVIL. AÇÃO CIVIL PÚBLICA. PRELIMINARES. FALTA DE INTERESSE DE AGIR. REJEITADA. NULIDADE DA SENTENÇA. CERCEAMENTO DE DEFESA. VÍCIO DE FUNDAMENTAÇÃO. REJEITADAS. MÉRITO. DADOS PESSOAIS. AMPLA PROTEÇÃO NORMATIVA. DIREITO FUNDAMENTAL. DIREITO À PRIVACIDADE. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. LGPD. RECURSO CONHECIDO E NÃO PROVIDO. DECISÃO MANTIDA. 1. O fato de o réu apelante ter excluído o anúncio e o site onde negociava dados pessoais de terceiros, não esvazia o pedido do autor, consistente na pretensão de que haja abstenção, pelo réu apelante, da disponibilização de dados pessoais de terceiros. Preliminar de falta de interesse rejeitada. 2. As alegações de cerceamento apresentadas pelo apelante são genéricas e não indicam qual prejuízo teve o apelante, não havendo que se falar em cerceamento de defesa. Preliminar de cerceamento de defesa afastada. 3. O magistrado, no exercício de sua atividade jurisdicional, não precisa discorrer pontualmente a respeito de todas as questões e dispositivos de lei suscitados pela parte para cumprir com plenitude a devida prestação jurisdicional, sendo certo que deve declinar as razões de decidir, tal qual realizado nos autos. Preliminar de nulidade da sentença rejeitada. 4. A proteção aos dados pessoais está diretamente ligada ao direito à privacidade, que consta expressamente no rol dos direitos fundamentais da Lei Maior. Assim, a disponibilização de dados pessoais pode causar "danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários". Precedente do STF. 5. A Lei Geral de Proteção de Dados Pessoais - LGPD possui carga de agregar, isto é, sua positivação possui valor substancial de incrementar o atual ordenamento jurídico brasileiro, em nada obstando a tutela jurisdicional, amparada em outras normas, no que se refere à proteção de dados pessoais. 6. O Código de Processo Civil, em seu artigo 497, prevê que, em se tratando de obrigação de não fazer, deve o magistrado aplicar medidas coercitivas a fim de coibir a parte sucumbente à prática da conduta vedada. 6.1. No caso dos autos, a multa imposta pelo sentenciante não guardarelação com as sanções previstas na LGPD, que ainda carecem de aplicabilidade. 7. Recurso conhecido. Preliminares rejeitadas. No mérito, recurso não provido. Sentença mantida.

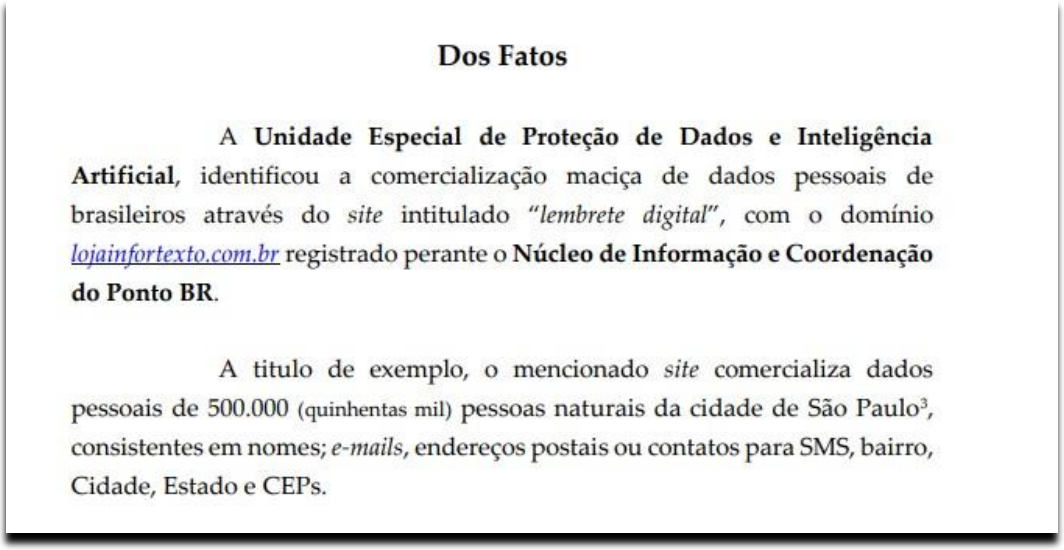
Ocorreu o recurso pelas partes, entretanto o magistrado seguiu com sua decisão:

> O Juízo da Décima Sétima Vara Cível de Brasília decidiu a lide nos seguintes termos: Ante o exposto, JULGO PROCEDENTE o pedido formulado na inicial para, confirmando a decisão de ID 74668327, determinar ao réu que seabstenha de disponibilizar, de forma gratuita ou onerosa, digital ou física, dados pessoais de brasileiros, sob pena de incidência de multa no valor de R$5.000,00 (cinco mil reais), para cada operação nesse sentido, sem prejuízo da adoção de outra medida, concomitante ou não, que se mostrar necessária. Em razão da sucumbência, o réu arcará com a totalidade das custas processuais. Sem honorários.

A Lei geral de Proteção de Dados está a menos de três anos em vigência, e também já foi alvo de fundamentação jurídica em uma Ação Civil Pública (ACP), em que o Ministério Público do Distrito Federal ajuizou uma ACP contra uma empresa de informática que comercializada dados pessoais de usuários, dados esses como nome, e-mail, contatos telefônicos, entre outros.

Para ilustrar a situação narrada, segue uma imagem contendo breve fatos alegado na ACP (2022, p. 2):

FIGURA 6 – ACP – DOS FATOS



Dos Fatos

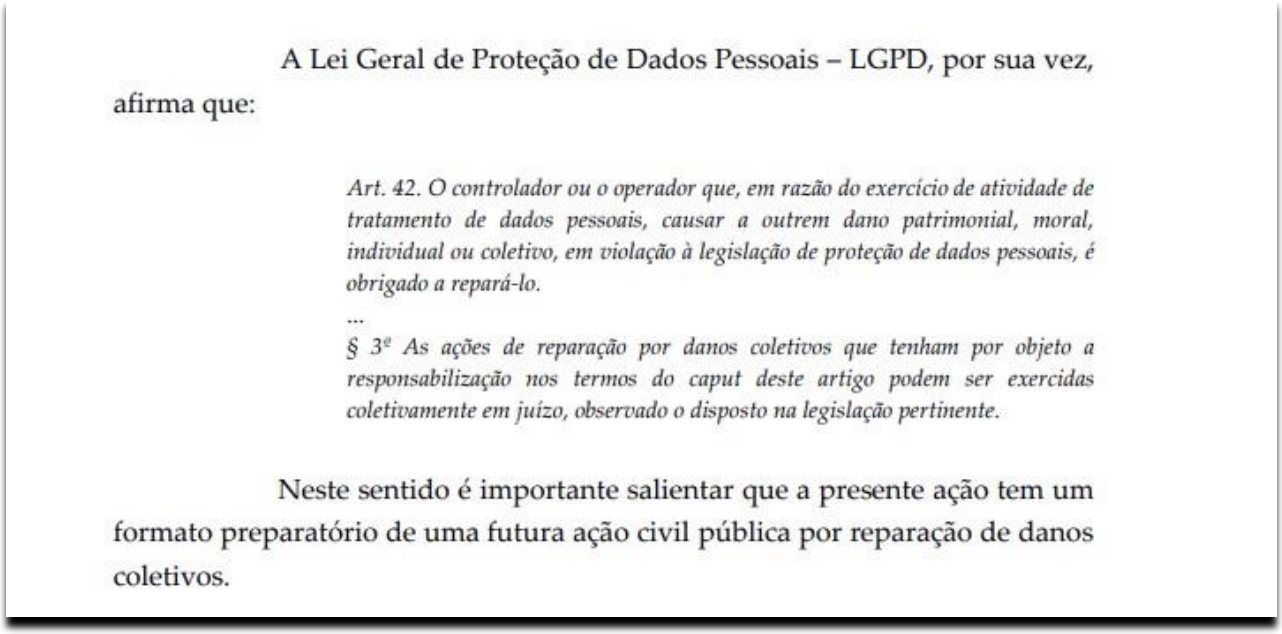
A **Unidade Especial de Proteção de Dados e Inteligência Artificial**, identificou a comercialização maciça de dados pessoais de brasileiros através do *site* intitulado *"lembrete digital"*, com o domínio *lojainfortexto.com.br* registrado perante o **Núcleo de Informação e Coordenação do Ponto BR**.

A titulo de exemplo, o mencionado *site* comercializa dados pessoais de 500.000 (quinhentas mil) pessoas naturais da cidade de São Paulo[3], consistentes em nomes; *e-mails*, endereços postais ou contatos para SMS, bairro, Cidade, Estado e CEPs.

Fonte: Ação Civil Pública. Ministério Público do Distrito Federal e Territórios Unidade de Proteção de Dados e Inteligência Artificial. Espec. Disponível em https://www.mpdft.mp.br/portal/pdf/Ac%CC%A7a%CC%83o_Civil_Pu%CC%81blico_-_Infortexto_-_MPDFT_-_XXXXXX.pdf

A comercialização realizada pelo site alvo da ACP, foi impactada em todos os entes federados. A fundamentação da Ação com base na Lei Geral de Proteção de Dados, apresentou-se na ACP, no capitulo Da Competência do Poder Judiciário do Distrito Federal e dos Territórios, em que o Ministério Público apresenta que (2022, p. 7):

Figura 7 – ACP – FUNDAMENTAÇÃO



A Lei Geral de Proteção de Dados Pessoais – LGPD, por sua vez, afirma que:

> *Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.*
> ...
> *§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.*

Neste sentido é importante salientar que a presente ação tem um formato preparatório de uma futura ação civil pública por reparação de danos coletivos.

Fonte: Ação Civil Pública. Ministério Público do Distrito Federal e Territórios Unidade de Proteção de Dados e Inteligência Artificial. Espec. Disponível em https://www.mpdft.mp.br/portal/pdf/Ac%CC%A7a%CC%83o_Civil_Pu%CC%81blico_-_Infortexto_-_MPDFT_-_XXXXXX.pdf

Além da fundamentação da referida ACP com a LGPD, ressalta-se que o Ministério Publica aciona a Constituição Federal de 1988, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet, Regulamento do Marco Civil da Internet, ou seja, todas legislações infraconstitucionais que já fora citada nos capítulos anteriores da distinta monografia, visto que são aparatos normativos que embasaram a criação da LGPD no Brasil.

Na Ação Civil Pública apresentada, fora realizado o pedido de tutela liminar de urgência, acrescentado do pedido de congelamento da funcionalidade do domínio do site que estava realizando a comercialização dos dados, site este com endereço: lojainfortexto.com.br, em que até a presente data da referida pesquisa ainda assim esta sendo mantido o seu congelamento. A referida Ação Civil Pública foi impetrada pelo

Promotor de Justiça Frederico Meinberg Coordenador da Espec, em 21 de setembro de 2020.

Ainda que a referida Lei, objeto da distinta pesquisa, tenha se apresentado em tamanha relevância em nosso ordenamento jurídico brasileiro, e que há total fundamento para não ser utilizada como uma lei complementar, ainda assim que em alguns processos,e jurisprudências a mesma não tem sido citada como principal fundamento jurídico, a LGPD tem sido citada como um mecanismo de reforço a alguma outra legislação.

Ou seja, observa-se que a LGPD ainda possui um longo caminho a ser percorrido para que consiga materializar o status de Lei que possui, e assim deixe de ser citada como Lei complementar para solucionar as lides levadas aos tribunais brasileiros, em especialno cenário tecnológico atual, visto que as normativas que tínhamos antes da promulgação da LGPD contemplava a intimidade e ao sigilo de comunicações, mas não atendiam as relações da sociedade digital, o que acarretava em um negligencia no tratamento de dados.

4.1 STF e a tendência da Fundamentalidade da Proteção de Dados

A relevância da Lei Geral de Proteção de Dados no ordenamento jurídico brasileiro, tem alcançado uma crescente importância, em especial no reconhecimento do tratamento de dados pessoais como direito fundamental, a qual ocorreu no ano de 2020, em que Supremo Tribunal de Justiça já tinha o posicionamento de que a proteção de dados tinha que ser compreendida como status de direito fundamental.

Essa conquista foi possível a partir da decisão embasado no entendimento do Ministro Gilmar Mendes que votou para suspender a MP 954 que obrigava que algumas empresas de telefonia realizasse o repasse de informações ao IBGE sobre dados pessoais de seus consumidores. Tratava-se apenas de uma MP que solicitava tais informações de cunho pessoal, sem ao menos esclarecer qual o objetivo e destinação do angariamento dessas informações.

A partir do entendimento do Ministro, o plenário referendou "a Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6393, 6390, suspendendo a aplicação da Medida Provisória 954/2018" (DUARTE, s.p, 2020).

Esse julgamento adentrou a um marco histórico no âmbito legislativo, visto que fundamenta a tutela a proteção aos dados pessoais como direito fundamental, em que o STJ entendeu ser necessário uma proteção de modo que não se torna a vigilância uma

regra na vida do indivíduo, de modo que indiretamente limitasse liberdades conquistas em um longo período, ocorrendo assim um desmonte silencioso de direitos conquistados.

Como bem reforça a Ministra Rosa Weber (2018) em seu voto:

> [...] a história nos ensina que uma vez estabelecida a sistemática de vigilância, há grande perigo de que as medidas não retrocedam e que os dados já coletados sejam usados em contextos muito diversos daquele que justificaram inicialmente a sua coleta.

A LGPD e o reconhecimento da proteção de dados como um direito fundamental, proporciona uma forma inédito de inovação no ordenamento jurídico brasileiro, ressaltando que não existe mais dados irrelevantes, todo dado é fundamental e deve ser protegido.

> Fazendo referência ora ao acórdão da Corte constitucional alemã, ora ao direito da Carta de Direitos Fundamentais da União Europeia (art. 8º), os Min. Rosa Weber, Gilmar Mendes e Luiz Fux trataram de um direito fundamental à proteção de dados pessoais garantido pela Constituição Federal. Nesse sentido, percebem-se indícios de que se trata de um direito autônomo, que se diferencia da proteção à intimidade e privacidade, vez que o objeto protegido é distinto. Com a ascensão de métodos sofisticados de processamento e tratamento de dados pessoais, carregando consigo riscos maiores para a personalidade do cidadão, esse direito ganha contornos próprios, nos termos do voto do Min. Gilmar Mendes: A autonomia do direito fundamental em jogo na presente ADI exorbita, em essência, de sua mera equiparação com o conteúdo normativo da cláusula de proteção ao sigilo. A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa. (ALVES DUARTE, 2020, s.p.)

A proteção de dados, hoje reconhecida como um direito fundamental, abrange o âmbito de proteção subjetivo do cidadão, no sentido de defender a liberdade individual do indivíduo, de modo que delimite a intervenção estatal, bem como o âmbito objetivo no que fiz respeito a ações do Estado de proteção e garantia desse direito nas diversas esferas, publica ou privada, ou seja, uma garantia de controle do próprio Estado para com si próprio sobre sua ação ou omissão no que fiz respeito a esse direito.

4.2 Emenda Constitucional 115 de 2022 e a Proteção de Dados como Direito Fundamental

O Congresso Nacional aprovou a Emenda Constitucional 115 de 2022, a qual: "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais." EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022.

A referida Emenda oficializa diante do ordenamento jurídico brasileiro a proteção dos dados como um direito fundamental, acrescentando a seguinte redação: LXXIX, com a previsão de que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais".

Além desse reconhecimento e inclusão no texto normativo, a referida Emenda acrescenta no artigo 21 da Constituição Federal de 1988, a seguinte redação: "XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. (Incluído pela Emenda Constitucional nº 115, de 2022)", e estabelece que a União possui competência para legislar sobre a temática.

O reconhecimento da proteção de dados como um direito fundamental, infelizmente não é uma inovação legislativa brasileiro, já existiam precedentes de outros países, como a Alemanha que adotou o mesmo entendimento:

> Apesar de estar contido implicitamente em normas constitucionais, o prévio reconhecimento da proteção de dados como direito fundamental pelo STF e a sua recente positivação constitucional colocam o Brasil ao lado de outras experiências internacionais positivas no tratamento do tema. Cumpre destacar que, desde 1983, o Tribunal Constitucional Federal da Alemanha já considera a proteção de dados como um direito fundamental a partir do julgamento de reclamações constitucionais ajuizadas contra o recenseamento geral da população determinado pela Lei do Censo daquele ano (VOLKSZÄHLUNGSURTEIL, 2022, s.p.).

Na época, o Tribunal Alemão, compreendeu que em virtude dos avanços na sociedade tecnológica o processo de armazenamento de informação por meio de dados, estava acontecendo de forma desenfreada, surgindo assim a necessidade de o Tribunal Alemão acompanhar essas mudanças e garantir a proteção a possíveis ameaças, interpretando a proteção dos doados como um direito fundamental.

> O Tribunal de Justiça da União Europeia, no dia 13 de maio de 2014, proferiu a histórica decisão de reconhecer a existência de um direito a apagar dados pessoais na internet, o que se denomina em inglês de right to erasure. Diferentemente do que se tem afirmado em alguns textos jornalísticos e jurídicos, mais do que admitir a existência de um direito a ser esquecido (right to be forgotten, embora seja mais popular a expressão "direito ao esquecimento"), o tribunal europeu foi além e passou admitir o senhorio da pessoa sobre seus dados disponíveis na rede (JUNIOR, 2014, s.p.).

Ou seja, já havia precedentes para a referida alteração jurídica brasileira, a qual através da Emenda Constitucional 115 de 2022, tornou-se possível explicitar a relevância crescente da proteção dos dados, como um direito fundamental, agora sacramentado em nossa Constituição Federal.

A distinta Emenda, sem dúvida alguma proporcionou um reforço no que diz respeito a liberdade dos cidadãos e proteção a seus direitos em relação a privacidade, atingindo a esfera digital e a informatização e propagação instantânea de dados, com um acréscimo, hoje tal direito está constituído como um direito fundamental com status de cláusula pétrea, sendo vedado qualquer alteração que reduza a proteção constitucional conferida a esse direito.

5 CONCLUSÃO

A referida monografia, teve por objetivo proporcionar reflexões e análise sobre o cenário em que se consolidou a LGPD, sob o ponto de vista crítico da distinta legislação, que sem sombra de dúvidas é um grande avanço e inovação normativa.

Sob essa ótica, foi possível elucidar a teoria de vigilância, monitoramento, tratamento e direcionamento de dados, bem como, a compreensão de que esses dados são o "novo petróleo do século XXI, ou da sociedade 4.0",, hoje já conhecida como sociedade 5.0, visto que a quantidade de dados extraídos de uma breve navegação pode definir inclusive os aspectos psíquicos daquele navegante.

Ocorre que todas essas mudanças sem sombra de dúvidas impactam as esferas políticas, sociais o que automaticamente traz influencias nas relações jurídicas, e no âmbito da esfera jurídica podemos citar os negócios jurídicos nessa sociedade sem barreiras.

Ressalta-se também que embora a distinta normativa tenha adentrado no ordenamento jurídico a partir de uma complexa e longa construção, ainda assim a mesma somente se consolidou como uma exigência indireta da União Europeia, em que determinou que somente manteria relações econômicas com aqueles países que já tivessem implementado uma normativa que trata-se especificamente da proteção de dados, diante disso, temos esse fato como exemplo de um dos diversos impactos na esfera política, a relacional entre Brasil e União Europeia.

Ainda que a LGPD tenha por princípios o zelo e proteção jurídica dos dados dos indivíduos, ainda assim há uma trajetória jurídica a ser percorrida e delimitada, visto que na sociedade 4.0 esses dados devem ser protegidos em esferas distintas, inclusive na digital, destacando que essa tecnologia está em constante transformação. Há necessidade de metodologias especificas para cada meio de circulação de dados, seja na esfera física, seja na esfera digital. Destaca-se que na sociedade pós-moderna, o acesso à informações é amplamente facilitado e isso demanda uma proteção cada vez mais efetiva dos dados pessoais dos cidadãos.

A promulgação de uma Lei de Proteção de Dados por si só já materializa um a grande avanço no âmbito jurídico, mas o reconhecimento dessa proteção como um direito fundamental, sem sombra de duvidas proporcionou uma legitimidade inalienável e imprescritível, ou seja, não se discute a possiblidade de revogação do feito, visto que os direitos fundamentais são prerrogativas reconhecidas pelo Estado.

Ressalta-se que a evolução dos direitos fundamentais deve acompanhar as mudanças na sociedade, e com a revolução digital não seria diferente, dessa forma a LGPD vem justamente para proporcionar segurança jurídica a institutos que não estavam sendo tutelados pelo Estado, de forma efetiva, direitos como sigilo pessoal no que tange os dados pessoais, com ênfase naqueles dados coletados de pesquisas acessadas através meio das plataformas digitais.

Há um longo caminho a ser percorrido, estudado, analisado e implementado, em especial na reeducação legislativa da sociedade para recepcionar a LGPD, mas sem sombra de dúvidas essa normativa contempla excelentes estratégias para proteção da individualidade e privacidade do indivíduo, contribuindo assim para a materialidade da segurança jurídica.

REFERÊNCIAS

ASSEMBLEIA GERAL DA ONU (1948). **Declaração Universal dos Direitos Humanos.** Disponível em https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em 22 de agosto de 2022.

BRASIL Ação Civil Pública. **NÚMERO DA AÇÃO** Ministério Público do Distrito Federal e Territórios Unidade de Proteção de Dados e Inteligência Artificial. Espec. Disponível em https://www.mpdft.mp.br/portal/pdf/Ac%CC%A7a%CC%83o_Civil_Pu%CC%81blico_-_Infortexto_-_MPDFT_-_XXXXXX.pdf. Acesso em 12 de outubro de 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República [2022]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 10 de abril de 2022.

BRASIL. **Código de Defesa do Consumidor.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 14 de abril de 2022.

BRASIL. **Código Penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 14 de abril de 2022.

BRASIL. **Lei Geral de Proteção de Dados.** LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 12 de abril de 2022.

BRASIL. **Emenda Constitucional 115 de 2022.** Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais.. Acesso em 26 de outubro de 2022.

BRASL. **Lei nº 13.853, de 8 de julho de 2019.** Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em 10 de outubro de 2022.

BRASIL. **Processo 07337853920208070001 - (0733785-39.2020.8.07.0001 - Res. 65 CNJ)** Mendes, relator: Rômulo de Araújo **.** 1ª Turma Cível. Disponível em https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj. Acesso em 12 de outubro de 2022.

BRASIL. **Lei nº 14.010, de 10 de junho de 2020.** Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em 10 de outubro de 2022.

BRASIL. **Portaria nº 213, de 15 de outubro de 2020.** Disponível em https://www.stj.jus.br/internet_docs/biblioteca/clippinglegislacao/Prt_213_2020_CNJ.pdf. Acesso em 10 de outubro de 2022.

BRASIL. **Portaria nº 213, de 15 de outubro de 2020.** Disponível em https://www.stj.jus.br/internet_docs/biblioteca/clippinglegislacao/Prt_212_2020_CNJ.pdf. Acesso em 10 de outubro de 2022.

BRASIL. **Portaria nº 212, de 15 de outubro de 2020.** Disponível em https://www.stj.jus.br/internet_docs/biblioteca/clippinglegislacao/Prt_212_2020_CNJ.pdf. Acesso em 10 de outubro de 2022.
PORTARIA Nº 213, DE 15 DE OUTUBRO DE 2020. Disponível em https://www.stj.jus.br/internet_docs/biblioteca/clippinglegislacao/Prt_213_2020_CNJ.pdf. Acesso 10 de outubro de 2022.

BRASIL. **Portaria stj/gdg n. 178 de 12 de março de 2021.** Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/151625. Acesso em 24 de setembro de 2022.

BRASIL. **Recomendação Nº 73 de 20/08/2020.** Disponível em https://atos.cnj.jus.br/atos/detalhar/3432. Acesso em 10 de outubro de 2022.

BRASIL. **Resolução Nº 334 de 21/09/2020.** Disponível em https://atos.cnj.jus.br/atos/detalhar/3489. Acesso em 10 de outubro de 2022.

BRASIL**. Resolução Nº 363 de 12/01/2021.** Disponível em https://atos.cnj.jus.br/files/original181204202101196007 20f42c02e.pdf. Acesso em 08 de outubro de 2022.

CAMARA, Dennys Eduardo Gonsales. GHERINI, Pamela Michelena De marchi. GOMES, Maria Cecilia Oliveira. MONTEIRO, Renato Leite. MORIBE, Gabriela. NOVAES, Adriane Loureiro. **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos. 2018**. Disponível em https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em 15 de abril de 2022

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em 20 de agosto de 2022. de 24 de Outubro de 1995. Disponível em https://www.conjur.com.br/dl/diretiva-europeia.pdf. Acesso em 23 de agosto de 2022.

DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO. Disponível em https://www.conjur.com.br/dl/diretiva-europeia.pdf. Acesso em 12 de junho de 2022.

HIRATA, Alessandro. **Direito à privacidade.** Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 26 de maio de 2022.

EFFICIENCY OF JUSTICE (CEPEJ) **European ethical charter on the use of artificial intelligence in judicial systems and their environment**. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, December 3-4, 2018). Disponível https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Acesso em 15 de setembro de 2022.

EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ). European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018). Disponível em https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. Acesso em 17 de agosto 2022.

GRIMM, Dieter**. Persönlichkeitsschutz im Verfassungsrecht. In: *Karlsruher Forum 1996. Schutz der Persönlichkeit. Mit Vorträgen von Dieter Grimm und Peter Scherdtner***. Karlsruhe: Verlag Versicherungswirtschaft, 1997, p. 19 a 21.

JANONE, Lucas. **Quatro em dez empresas brasileiras agem contra vazamento de dados, diz pesquisa.** Disponível em https://www.cnnbrasil.com.br/business/quatro-em-dez-empresas-brasileiras-agem-contra-vazamento-de-dados-diz-pesquisa/. Acesso em 17 de agosto de 2022.

JUNIOR, Otavio Luiz Rodrigues. **Direito de apagar dados e a decisão do tribunal europeu no caso Google (Parte 2).** Disponivel em: https://www.conjur.com.br/2014-mai-28/direito-comparado-direito-apagar-dados-decisao-tribunal-europeu-google-espanha. Acesso em 18 de setembro de 2022.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18).** Disponível em https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em 19 de agosto de 2022.

MARCATO, Gisele Caversan Beltrami. **O Uso Inteligência Artificial na Prestação Jurisdicional Brasileira: Em Questão os Valores Éticos e Constitucionais..** Universidade Estadual do Norte Do Paraná Campus De Jacarezinho – Pr. Centro De Ciências Sociais Aplicadas Programa De Pós-Graduação Em Ciência Jurídica Doutorado, 2022.

MENDES, Laura. **Habeas Data e Autodeterminação informativa: dois lados da mesma moeda.** In: Direitos Fundamentais & Justiça, ano 12, n. 39, p. 185-216, jul./dez. 2018.

PRATES, Arthur Sousa Marx. **Comercialização de dados pessoais entre empresas privadas após a implementação da LGPD (Lei Geral de Proteção de Dados).**

Disponível em https://conteudojuridico.com.br/consulta/Artigos/56819/comercializao-de-dados-pessoais-entre-empresas-privadas-aps-a-implementao-da-lgpd-lei-geral-de-proteo-de-dados. Acesso 28 de maio de 2022.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** Disponível em file:///C:/Users/Cliente/Desktop/LGPD/MATERIAIS/2%C2%BA%20Capitulo/O%20DIREITO%20A%20PRIVACIDADE%20NA%20SOCIEDADE%20DA%20INFORMA%C3%87%C3%83O.pdf. Acesso em 20 de julho de 2022.

PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018: uma análise dos principais aspectos e do conceito de privacidade na sociedade informacional.** Disponível em https://acervodigital.ufpr.br/bitstream/handle/1884/68114/TCC%20FINAL%20-%20lgpd.pdf?sequence=1&isAllowed=y. Acesso em 12 de agosto de 2022.

PEREIRA, Tullyo Gabriel Gontijo. PRATES, Arthur Sousa Marx. **Comercialização de dados pessoais entre empresas privadas após a implementação da LGPD (Lei Geral de Proteção de Dados)**. Disponível em https://jus.com.br/artigos/90903/comercializacao-de-dados-pessoais-entre-empresas-privadas-apos-a-implementacao-da-lgpd-lei-geral-de-protecao-de-dados. Acesso em 28 de maio de 2022.

PINTO, Douglas Guzzo. **A proteção de dados alçada a direito fundamental na Constituição brasileira**. Disponível em https://www.conjur.com.br/2022-fev-17/douglas-pinto-protecao-dados-alcada-direito-fundamental. Acesso em 25 de outubro de 2022.

SÁ, Marcelo Dias de. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas.: Aplicações mobile do governo**. Disponível em https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em 20 de agosto de 2022.

SANTI, Leandro**. Lei 13.709/2018: análise à lei geral de proteção de dados pessoais (lgpd).** Disponível em https://repositorio.animaeducacao.com.br/bitstream/ANIMA/6086/3/Monografia%20-%20Leandro%20Santi%20-%2024.06.2020.pdf. Acesso em 23 de abril de 2022.

SANTOS, Michelly. **Princípio da segurança jurídica..** Disponível em https://michellysantos.jusbrasil.com.br/artigos/171343529/principio-da-seguranca-juridica. Acessado em 10 de abril de 2022.

SANTOS, Viviane Bezerra De Menezes. **Lei geral de proteção de dados: fundamentos e compliance.** Disponível em

https://repositorio.ufc.br/bitstream/riufc/49370/1/2019_tcc_vbmsantos.pdf. Acesso em 03 de maio de 2022.

SANTOS, Viviane Bezerra de Menezes. **Lei geral de proteção de dados: fundamentos e compliance.** Disponível em: https://repositorio.ufc.br/handle/riufc/49370. Acesso em 22 de setembro de 2022.

SOUZA, Thiago Pinheiro Vieira De. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies. 2018.** Disponível em https://repositorio.ufu.br/bitstream/123456789/23198/3/Prote%C3%A7%C3%A3oDadosPessoais.pdf. Acessado em 06 de maio de 2022.

Tribunal de Justiça do Distrito Federal e dos Territórios. **LGPD: Justiça determina que site suspenda anúncio de venda de banco de dados cadastrais. Tribunal de Justiça do Distrito Federal e dos Territórios**. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/outubro/justica-determina-que-site-suspenda-anuncio-de-venda-de-banco-de-dados-cadastrais

VITAL, Danilo. **Gilmar: Pandemia não atenua, mas reforça necessidade de proteção de dados**. Disponível em: https://www.conjur.com.br/2020-mai-07/pandemia-reforca-necessidade-protecao-dados-gilmar Acesso em: 9 de maio de 2020.

O'NEIL, Cathy. **Weapson Of Math Destruction. How Big Date Increases Inequality And Threatens Democracy Cathy O' Neil.**